Find out more
www.thebci.org

bci Thought Leadership

BCI Emergency & Crisis Communications Report 2024

F24

bci Leading the way to resilience

Contents

7 Executive summary

14 The toolbox

43 Tool requirements

50 Activation of plans: triggers, response levels, and timing

70 Key challenges

82 Building resilience: training and exercising

92 Internet of Things (IoT)

100 Annex

Foreword

We are pleased to present the tenth anniversary edition of the BCI Emergency & Crisis Communications Report. We would like to thank F24 for their longstanding sponsorship of this vital report in the BCI's Thought Leadership portfolio.

This year's report not only looks back at changes, trends, and concerns relating to emergency and crisis communications, but also reviews the macrotrends of the past decade. There have been a number of world-shaping events that have occurred over the past ten years which have influenced the way organizations communicate: the pandemic, for example, prompted a shift to remote working which has lessened the requirement for onsite, one-way communication. Meanwhile, global conflicts have heightened the challenges of being able to communicate when staff become displaced and increasing climate-related events have showcased the need for backup communication solutions to be in place when network infrastructure fails.

Technology is also advancing at a rapid rate, and the use of desktop computers and laptops in crises is waning, and smartphones — with their increased functionality and processing power — are, in many situations, entirely replacing the need to use a computer. With this shift in usage, organizations are continuing to move away from desktop installed software (14.3% usage) towards software-as-a-service (SaaS) solutions. The data in this report shows that SaaS, or a hybrid SaaS/installed solution, speeds up activation times, while also providing multi-platform functionality.

It is encouraging to see that emergency communications providers are adapting to the asks of their customers and the last two years has seen a rise in organizations using hybrid installed software/SaaS solutions. By using existing systems to integrate with the features of a specialist tool, users can benefit from the improved functionality of dedicated software, while retaining user familiarity of their existing tool. In an era where training and exercising time can be hard to acquire, ease-of-use can be the tipping point between success and failure.

Indeed, this report highlights that the majority of failed activations are as a result of people failure, rather than that of systems. Lack of response from recipients was the cause of nearly two-thirds (62.3%) of failures, lack of accurate staff contact information for 41.0%, and a lack of understanding about what to do in an emergency at over a third (35.8%). Each of these are issues which can be lessened — or even fully resolved — by increased training and exercising. Encouragingly, this year's data shows that training and exercising of crisis communication plans is at an all-time high, with nearly 80% reporting training programmes take place once a year or more, with 75% saying plans are exercised once a year or more. Furthermore, organizations are more likely to train or exercise more than once a year too. With this increased diligence, we are hopeful that some of the human errors causing plan failure can be reduced over the next year.

We hope that this report provides a useful benchmarking document for organizations who already have a tool in place. For those who do not yet have a system in place or are considering a new solution, we hope it provides an awareness of the criteria that need to be considered when developing a new emergency and crisis communications system, as well as writing the training and exercising programmes to accompany it.

We would once again like to thank F24 for their continued sponsorship of this report and also offer our sincere thanks to everyone who completed the survey or participated in interviews for the report, both for this year and the past ten years. Data is only one part of the analysis process and the interviews help us to really understand the issues faced by practitioners in their day-to-day roles.

Rachael Elliott
Head of Thought Leadership
The BCI

F24

Foreword

Looking back on the developments of the past year, 2023 has once again put the resilience of companies to the test. Amid these crises, it is clear that the importance of resilience has grown beyond the status of a mere buzzword. The integration of resilience as a fundamental element of corporate strategy will continue to be crucial - as the results of this report clearly show.

Overall, it is encouraging to see that an increasing number of companies are taking these developments seriously by implementing appropriate measures to strengthen their resilience. The number of companies using software-as-a-service (SaaS) tools during a crisis, either as a standalone solution or coupled with on-premises installed software, is higher than ever before at 85.7%.

The evolution of software functionalities still aligns closely with the persisting challenges faced by organizations over the past years. From rapid alerting and mobilisation of a large workforce to comprehensive crisis handling, including task management, reporting, and status updates, and ensuring employee safety, particularly for lone workers, the versatility of these tools remains pivotal in navigating the intricacies of today's business landscape.

A noteworthy shift in trend has been observed in the reasons cited for not adopting or not planning to adopt dedicated tools for emergency communications and crisis management. While budgetary constraints held the top position in previous years, this year's report witnesses a significant drop, chosen by only 14.7% of respondents (compared to 34.8% in the 2023 report). This notable decrease of 20 percentage points signals a positive development, indicating that companies are increasingly recognising how crucial it is to invest in tools that enhance their crisis management capabilities.

Another particularly encouraging trend emerges when examining organizations' commitment to regular emergency communications training and exercising. This report shows an all-time high of almost 80% of organizations now running a scheduled training program. This underlines the increasing recognition of the need for ongoing skills development and preparedness.

Taking a holistic view, it is heartening to observe, as substantiated by the findings of this report, that an increasing number of companies are earnestly addressing these evolving challenges. At F24, we remain steadfast in our commitment to aid businesses on their resilience journey by providing dependable and cutting-edge software solutions.

As we celebrate the 10th anniversary of the BCI Emergency & Crisis Communications Report, it is a testament to a decade of collaborative efforts aimed at fostering a deeper understanding of the evolving dynamics in emergency and crisis communications. We at F24 are delighted to extend our longstanding partnership with the BCI and to contribute to their ongoing research efforts as a sponsor for the past six years. Our trust in this collaboration stems from the belief that organizations globally stand to obtain valuable insights from the latest data, gaining a comprehensive understanding of the current state of emergency notification systems and preparedness within companies. This knowledge, we anticipate, will be instrumental in shaping effective strategies for navigating crises and strengthening the resilience of companies.

Having said that, I hope you enjoy reading this report and gain a plethora of new and interesting information from it!

Benjamin Jansen
Senior Vice President Sales ENS/CM
F24

Executive summary

Mobile phones consolidate their position as the primary tool for the management of emergency communications

With remote and hybrid working becoming the norm, the ever-increasing functionality of mobile phones, combined with the expansion of software-as-a-service (SaaS) solutions available, mobile phones are now the preferred device to use in crisis situations. Software is also being more widely developed for mobile phones rather than tablet devices, with most providers optimising their software for use on smaller screens.

The tough economic climate means that organizations are seeking alternatives to investing in new tools

There has been a decline in investment in crisis management tools over the last twelve months, highlighting the tough financial environment that many organizations are operating within. Often, organizations are trying to find a workable balance between their requirements and budgets available by leveraging hybrid solutions which, in some cases, can combine existing on-site technology applications with new SaaS solutions.

Levels of dissatisfaction with emergency communications tools reach an all-time high

As the working environment becomes more complex, so do the requirements of crisis and emergency communications tools. As organizations opt for more cost-efficient solutions or delay upgrades, satisfaction levels have dropped. As such, almost two thirds of practitioners report being unhappy with their current tool. The main reasons for the dissatisfaction are the lack of integration with realistic alerting scenarios and the limited functionality of certain tools.

Practitioners are now more aware of the need to ensure that communications can continue if networks are down

As emergency communications solutions become increasingly reliant on network availability, professionals are becoming more aware of this as a key vulnerability of platforms. This is particularly relevant given the grandfathering of PSTN networks, set for around 2035 globally, which means that voice traffic will all be transferring to voice-over-IP (VoIP) solutions.

The human element remains the primary reason for failure of emergency communications plans

The predominant cause of breakdown in crisis communication plans in the 2024 report is the absence of response from recipients, chosen by 63.4% of respondents. The second most prevalent reason, chosen by 41%, is the lack of staff contact information. Additionally, in third place at 35.8% is the lack of understanding about what to do in a crisis. This shows that, despite high levels of training and exercising taking place, more still needs to be done to ensure that staff are fully briefed on the steps to take during an emergency.

The number of organizations undertaking regular training of their emergency communications is at a historic high

Nearly 80% of organizations now have a regular scheduled training programme for their emergency communication procedures. Furthermore, reserving training to a once-in-a-year activity is now falling out of favour: two in five organizations now train their staff between two and ten times a year.

Top five devices used to manage emergency communications

1 **92.5%** Mobile phones

2 **89.5%** Computers/laptops

3 **26.9%** Walkie-talkies/radios

4 **23.9%** Tablets **23.9%** Desk phones

5 **14.9%** Public address systems

Top five methods of communication used to activate the crisis team

1 **46.7%** Emergency communications management software

2 **40.7%** A tool which has been developed in-house

3 **35.3%** Crisis telephone lines

4 **28.7%** A secure messaging app dedicated for use within critical situations

5 **28.1%** Manual call trees

Software-as-a-service continues to be the standard for emergency and crisis communications software, either as a standalone tool or in hybrid schemes

Type of emergency/crisis management software used

61.1% We use a software-as-a-service (SaaS) solution

24.6% We use a hybrid model (combination of premises & SaaS solution)

14.3% We use on-premises installed software only

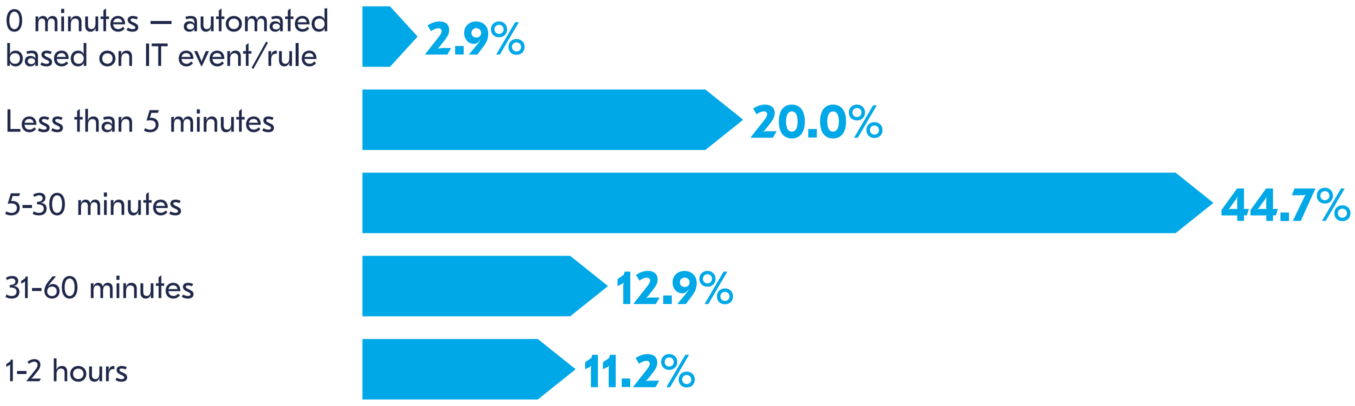
Practitioner dissatisfaction with tools of choice is at an all-time high

Are you happy with the solution you are currently using?

☺	😐	☹
30.7% Yes	**49.1%** Yes, somewhat	**20.2%** No

Organizations are taking longer to activate their plans because of the need to provide detailed and corroborated information to management

On average, how long does it take to activate your emergency or crisis communications plan?



Plans can be initiated faster if dedicated tools or software is used

Activation of emergency/crisis communication plans with and without the use of emergency communication tools

	Organizations using an emergency communication tool	Organizations not using an emergency communication tool	% difference of those using a tool vs those who do not
Organizations capable to activate plan within **5 minutes**	25.3%	17.0%	+8.3%
Organizations capable to activate plan within **30 minutes**	72.7%	57.6%	+15.1%

Lack of up-to-date staff information and limited understanding of what to do in a crisis are the primary reasons for plan failure

Top five reasons for not achieving the expected response levels

1	63.4%	Lack of response from staff/recipient
2	41.0%	Lack of accurate staff contact information
3	35.8%	Lack of understanding from recipients
4	34.3%	Staff device(s) were switched off/unavailable
5	23.1%	Failure of manual processes

Increasing severe weather events means that this has become the top reason for plan activation in the last twelve months

Top five triggers for emergency communications plans in the last 12 months

1	48.3%	Adverse weather
2	40.7%	IT or telecoms incident
3	35.6%	Cyber security incident or data breach
4	26.3%	IT incident
5	9.5%	Flood

Organizations are increasingly recognising the importance of performing training and exercising

In the last twelve months, almost 80% of organizations have implemented regular emergency communications training programmes. Furthermore, most organizations are now training and exercising more than once a year.

How often do you set up **training** programmes for your emergency or crisis communications plans?

48.7%	2-12 times a year
30.7%	Once a year

How often is your emergency or crisis communications plan **exercised**?

39.4%	2-12 times a year
36.0%	Once a year

Introduction

The BCI Emergency & Crisis Communications Report 2024 reflects on organizations' ongoing development of emergency and crisis communications strategies. With 2024 marking the tenth anniversary of this report, this year's analysis delves into trends noted over the past decade, as well as documenting more contemporary trends through this year's survey and face-to-face interviews. The characteristics and challenges identified in the 2023 report have continued to shape the landscape of the emergency and crisis communications space, with new developments and opportunities emerging in response to the evolving global context.

In the aftermath of the pandemic period, organizations have solidified remote working practices as the norm. This shift has prompted a re-evaluation and remodelling of emergency and crisis communications strategies to align with the demands of decentralised work environments. Many organizations have invested in new products and services to enhance their capabilities in an emergency scenario, while others are seeking more economical solutions and exploiting the functionality of their incumbent software to cope with budgetary restrictions.

A positive trend highlighted in the report is the consistent uptake of technology in crisis communications over the last ten years. Software-as-a-service (SaaS) solutions and hybrid models are becoming the norm, enabling fast activation of emergency and crisis communications plans. Collaboration features are also taking an increasingly important role in crisis communications, reflecting how one-way communications are no longer adequate for most organizations. It is this, coupled with the adoption of remote or hybrid working models, that is influencing the types of features that organizations are requesting for their crisis communication tools and technologies.

Challenges do persist, however, and human factors remain the cause of most failures in emergency communications plans. Nevertheless, the report notes an encouraging trend in the frequency and intensity of training and exercising initiatives that organizations are running to address this issue. Efforts are also underway to better integrate new technologies into crisis communications plans to minimise human errors when initiating plans.

Issues such as maintaining up-to-date staff contact details and data silos continue to pose significant challenges to organizations, even though there have been positive changes noted in the last ten years. The use of spreadsheets for personnel data is still common and this leads to data protection concerns, data not being updated in a timely manner, and problems with version control. These issues are prompting organizations to seek more robust solutions.

The report stresses a cautious outlook for 2024. While the acute impacts of the pandemic have mostly subsided, new challenges are emerging. Organizations are demonstrating a keen appetite for embracing new technologies to further enhance the resilience of their emergency and crisis communications. However, the report data shows a slowdown in the use of more advanced solutions in preference for more budget friendly options, as organizations seek to maximise cost benefits from the emergency communications solutions.

1

The toolbox

The toolbox

- Mobile devices and computers/laptops are the primary tools for the management of emergency communications. However, organizations are increasingly using a multi-tooled approach to suit the needs of the organization or the crisis being handled.
- SaaS tool usage is at an all-time high, either as a standalone solution or, increasingly, coupled with incumbent software through hybrid solutions.
- There has been a drop in investment in crisis management tools over the last twelve months, which reflects the challenging financial environment for many organizations.
- Smaller organizations and those with less cash reserves are seeking more cost effective solutions for their emergency communications needs.
- Organizations are expressing a historically high level of dissatisfaction with their emergency communications tools, indicating both a change in what practitioners demand from their tools, but also indicates that organizations may look towards new tools in 2024 as budgets open up.

This year's report shows that nearly two thirds of organizations (63.6%) use an emergency notification/crisis management tool or software to help them with their emergency communications plans — a 6.9% decrease from the figure in the 2023 report[1].

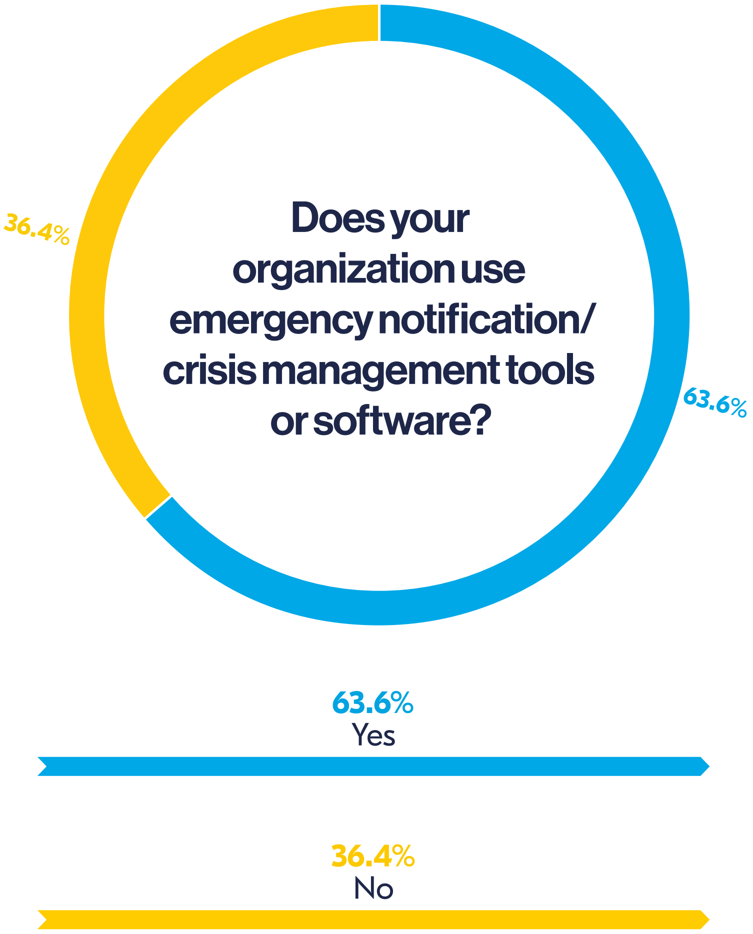
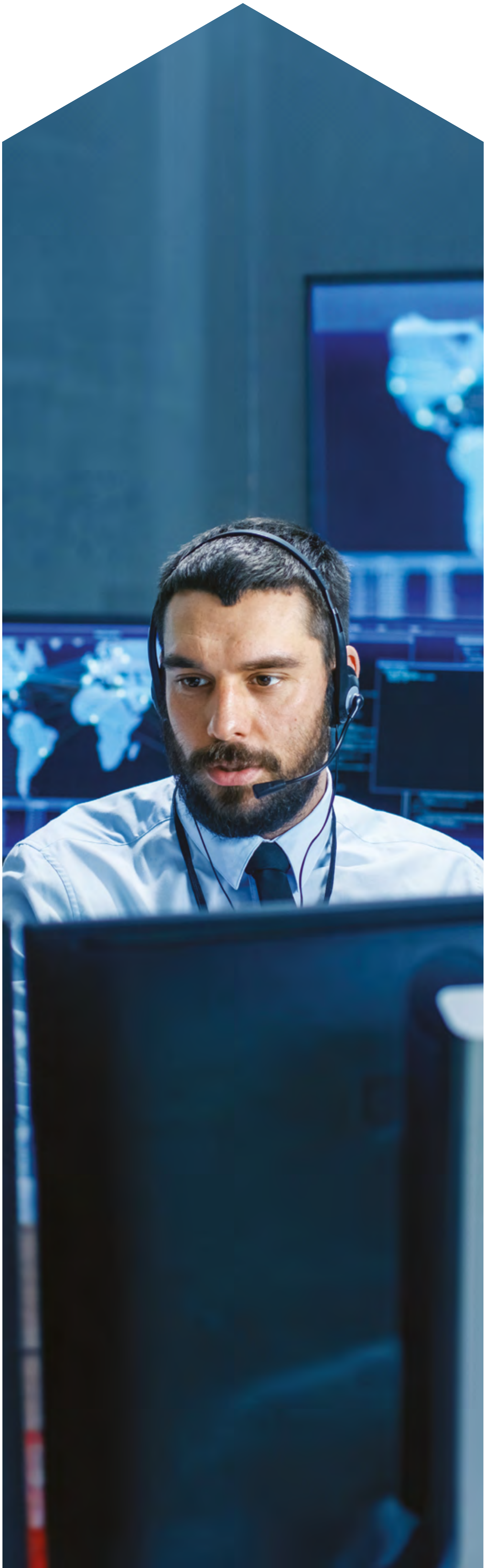


Figure 1. Does your organization use emergency notification/crisis management tools or software?



However, despite this year-on-year drop in tool usage, the historical data shows a rise between 2019 and 2024. Usage started to take off during the pandemic in 2020 as organizations invested in new solutions to assist with managing the COVID-19 pandemic, making further investments in the following years, peaking in 2023.

Usage of emergency notification/crisis management tools or software within organizations 2019- 2024

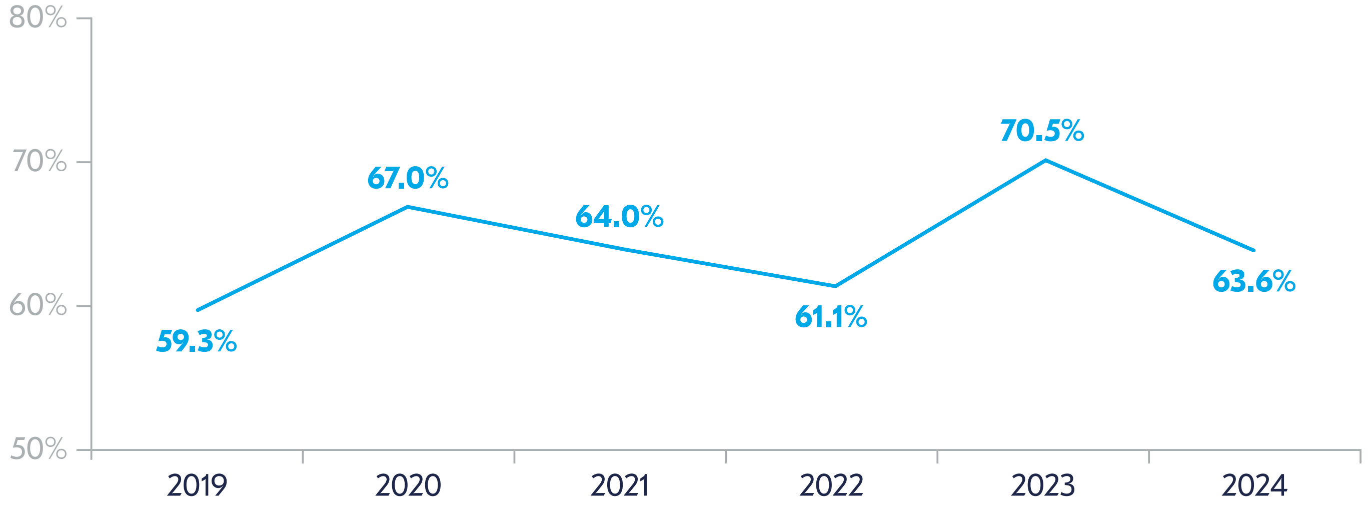


Figure 2. Usage of emergency notification/crisis management tools or software within organizations 2019-2024

Every year, practitioners are asked to identify the devices that are most commonly used during a crisis. The shift to remote or hybrid working setups prompted by the COVID-19 pandemic has led to a rise in the use of two-way communication tools (such as dedicated communications solutions) and a decline in the use of on-site and/or one-way communication tools (such as pagers).[2]

> **"Communication with a request for feedback is vitally important for our organization, especially if we're talking about out of hours because we won't have sight of people or other remote workers."**
>
> Emergency planning manager, health sector, UK

Some sectors have reverted to field/in-person operations, thereby prompting a resurgence of one-way communication modalities in corporate communication strategies. Nevertheless, as practitioners increasingly advocate for traceable communication, most crisis teams have adopted a more collaborative approach, with plans structured around remote or hybrid frameworks. The use of one-way communications and/or on-site communications is likely to track the diminishing role the office plays in corporate life[3], while simultaneously adapting other communication methods in use, to align with contemporary working patterns. However, one-way communications still have their place, particularly on sites which employ manual workers who frequently do not have access to a mobile phone during working hours, as well as sites such as university complexes where information transmission to students with multi-faceted preferences for communication can make electronic communication difficult.

The most frequently employed device in an emergency is the mobile phone (92.5%), taking the top position again this year. Mobile phones have been the tool of choice over the past three years, albeit showing a decline by 3.4 percentage points compared to the 2023 report. Nevertheless, its prominence at the top of list is indicative of the trend, already identified in previous reports[4], that mobile devices are becoming the incumbent tool within emergency contexts, driven by the proliferation of multiplatform software-as-a-service (SaaS) solutions, universal familiarity, and the continuously expanding capabilities of mobile telephones.

Laptops/computers remain in second place in the 2024 report, with 89.6% of respondents selecting this survey option. However, the proportion of individuals using laptops/computers has decreased by 4.4 percentage points year on year. This lowering trend has now been noted for a number of years from a high of 97.8% to its current value and points to a shift in usage to mobile devices due to the increased capabilities and availability of handsets.

Evolution of computer/laptop usage within emergency & crisis communications 2019-2024

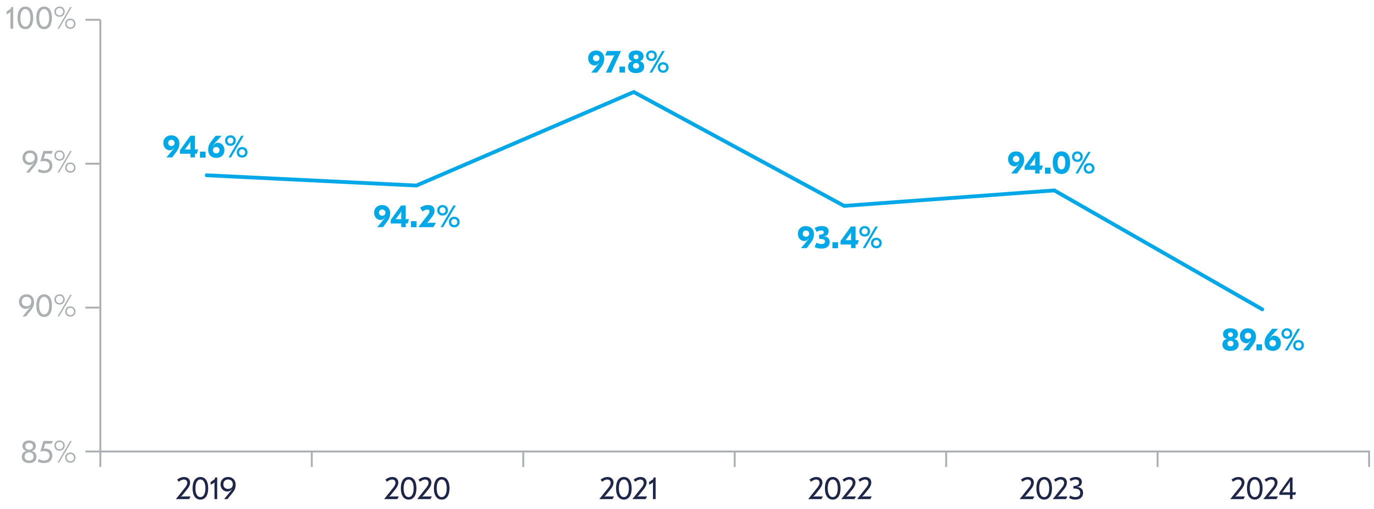


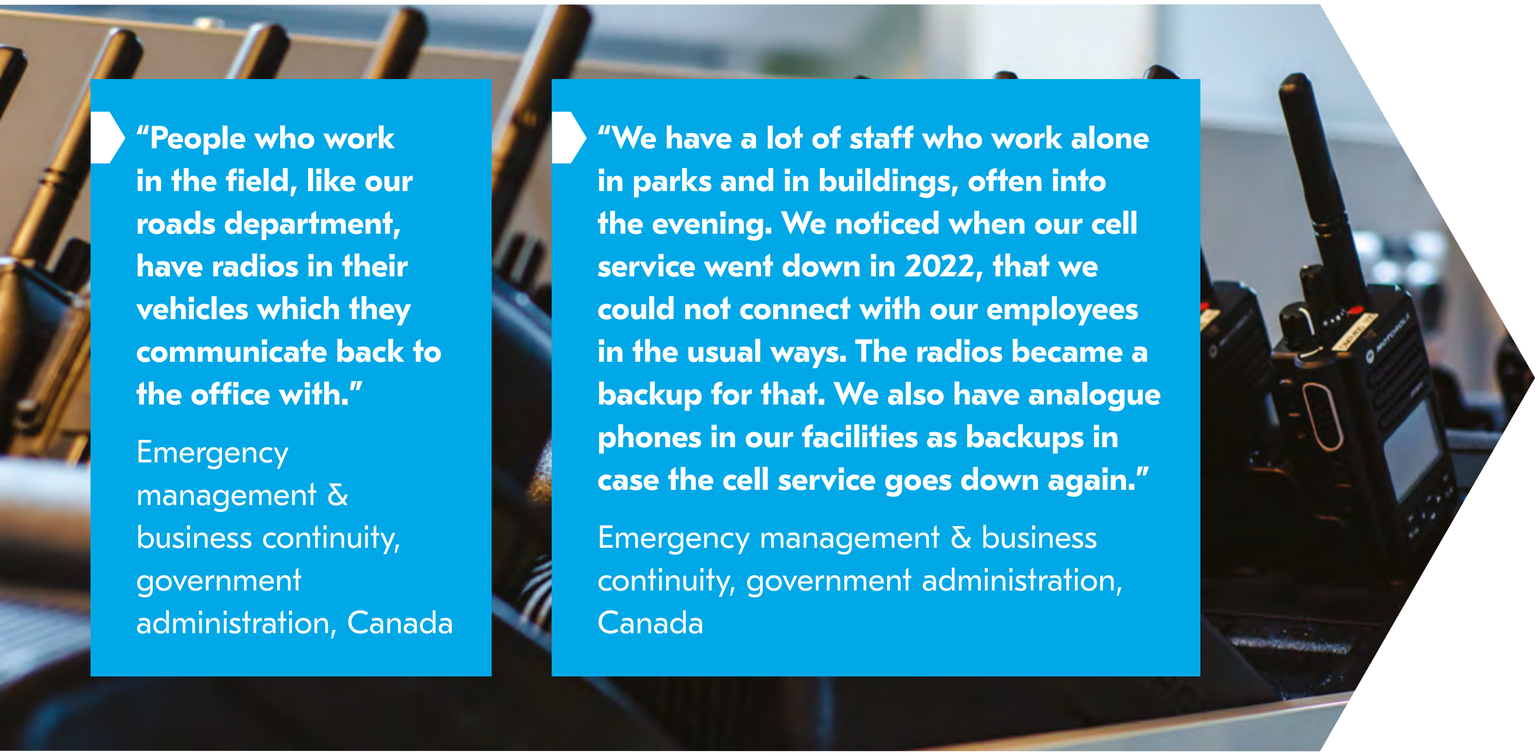
Figure 3. Evolution of computer/laptop usage within emergency & crisis communications 2019-2024

Despite the declining trend, a surge during 2021 is clear to see. This is likely to be explained by the COVID-19 pandemic and the many quarantines imposed by governments all over the world, where the majority of office workers switched to homeworking. During this time, computers became the main tool of communication for employees, with mobile phone calls dropping in favour of enterprise software such as Microsoft Teams. However, it is worth noting that the 2021 report (with data from 2020 — at the height of COVID-19) was the only time, within the period compared, that laptops and computers surpassed mobile phones as the prime tool of choice in emergency communications. Since then, the number of people using computers/laptops has seen a steady decline, with a -2.9% CAGR between 2021 and 2024.

The COVID-19 pandemic prompted organizations worldwide to adopt similar working practices in terms of remote working and devices used to adapt to this trend. In previous research[5], a respondent mentioned that their organization had to procure a set of new desktop computers, laptops, and mobile phones amid the COVID pandemic to facilitate remote work for the staff. The acquisition of this new equipment revitalised their emergency communication capabilities, as all new devices were configured with the same software. This uniformity allowed staff to communicate more efficiently, even when off-site.

After these two highly popular communication means, there is a significant drop-off to the more niche devices used for communication.

Walkie talkie and radio communication maintains its third position, being deployed in 26.9% of settings (2023: 27.7%). Typically radios and walkie-talkies are used by highly mobile on-site staff who need to communicate with colleagues, often when no WiFi or cellular network is available.



"People who work in the field, like our roads department, have radios in their vehicles which they communicate back to the office with."

Emergency management & business continuity, government administration, Canada

"We have a lot of staff who work alone in parks and in buildings, often into the evening. We noticed when our cell service went down in 2022, that we could not connect with our employees in the usual ways. The radios became a backup for that. We also have analogue phones in our facilities as backups in case the cell service goes down again."

Emergency management & business continuity, government administration, Canada

Even though the use of walkie-talkie/radios has increased momentum after falling significantly during the COVID-19 period (2021: 18.5%), levels of usage are still considerably below the numbers reported pre-pandemic (2020: 36.5%). However, radio communications continues to be considered essential for effective communication in many scenarios, especially in situations where all other forms of communication are unavailable.

Tablets and desk phones tie in fourth place with 23.9% of organizations using them. The use of desk phones reflects a continued decline in their popularity within office environments over the past five years (Figure 4). Therefore, this decline is not unexpected, especially when considering the new working landscape. In the wake of COVID-19, organizations have undergone substantial changes in their telecommunication systems and the switch to VoIP solutions is accelerating.

While the shift towards voice-over-IP solutions can result in cost-savings, it also introduces potential challenges. Unlike traditional phone lines, VoIP solutions depend on Internet connectivity for their operation which exposes organizations to the risk of unplanned downtime. In the event of an Internet outage, organizations and individuals using VoIP may find themselves without a means of communication, unless contingency plans are in place. An interviewee highlighted how this exact scenario happened within their organization.

No Internet Connection
Try these steps to get back online:
Check your modem and router
Reconnect to Wi-Fi
Reload Page

> **"Today, my personal home network went down. It was not the network that we use at work. However, I was without my personal internet all day today. At work, the alternative provider was going strong. It did provide a scare to say, well, what would happen if the whole network went down? What do we do next? I would not know how to alert everybody right now."**
>
> Business continuity, charity sector, Australia

Evolution of the usage of desk phones within emergency communications 2020-2024

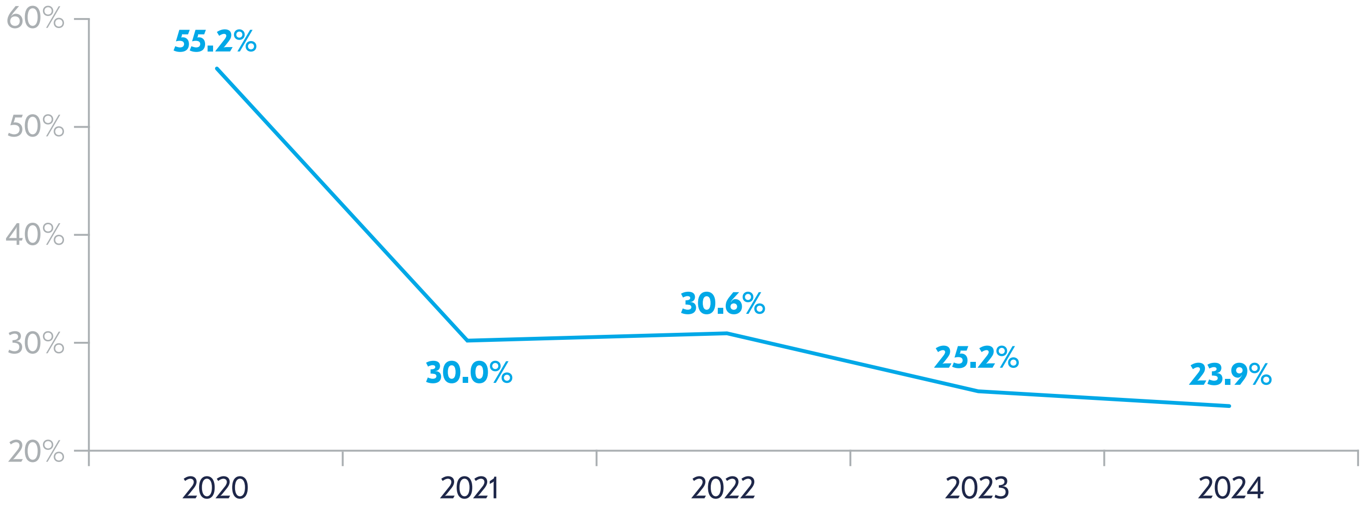


Figure 4. Evolution of the usage of desk phones within emergency communications 2020-2024

As the rollout of next-generation networks, such as fibre-optic, has gained momentum in the past five years, the issue of transitioning from outdated copper networks as decommissioning starts is growing in significance[6]. Countries worldwide exhibit varying approaches to phasing out old legacy systems. Some are actively pushing for the transition to modern telecommunication technologies, encouraging the abandonment of traditional infrastructure. Others however are adopting a more gradual or cautious strategy, considering factors such as rural connectivity, reliability concerns, and the potential impact on certain demographics. The policies and timelines for phasing out telephone copper lines also differ, reflecting the diverse challenges and priorities faced by nations.
As reported by Analysis Mason's Wireline Decommissioning Tracker[7], 16 operators globally have publicly declared the full cessation of their Public Switched Telephone Network (PSTN) services and five have successfully concluded the withdrawal of their copper services. Moreover, an additional 33 operators have communicated their plans or are currently in the process of phasing out copper services, with anticipated dates extending out to 2030. Based on this information, it is estimated that the majority of copper services will have undergone technical decommissioning by the year 2035. Some European nations, including the Netherlands, Estonia, and Germany, have already switched off the PSTN network and transitioned to IP phone networks already, while Norway, Spain, and Portugal are also making substantial progress. The UK's scheduled full switch-off is set to happen in 2025. Beyond Europe, Singapore has successfully switched off PSTN and both Japan and Australia are aiming to complete the transition by 2025. North America is working towards a non-PSTN future, however there is no hard deadline set to remove the existing PSTN service and the associated copper cable. India is in a similar position.

23.9% of respondents use tablets (2023: 23.6%) in crisis scenarios. The BCI Emergency & Crisis Communications Report 2023[8] documented the downward trend experienced in tablet usage, and this is likely to remain in the long term. As mentioned in last year's report, several factors contribute to this decrease in usage such as the substitution of tablets by laptop/tablet hybrids and the frequent absence of tablet-specific updates for certain applications. The tablet market has also been further influenced by the enhanced functionality of smartphones, which have grown in size, speed, storage, and capability, rendering tablet use in emergency scenarios as near to obsolete in some organizations. However, despite this trend, nearly a quarter of organizations still use tablets. An interviewee explained the use they give to tablets within their setting.

> **"We're not really using tablets. What we do try to do is encourage the use of applications on mobile phones. For example, we have a travel-related app for any travellers and it will give them warnings if an incident happens in their location."**
>
> Crisis management, financial services, USA

> **"Our outside workers use tablets to complete their checklists for their usual work. Therefore, we provide applications that they can use on these devices to report on events in the field in real time; it's just easier for them to use their tablets for these tasks, since they are already familiar with using them."**
>
> Emergency management & business continuity, government administration, Canada

Other tools being used in crises are public address systems (14.9%) and on-screen displays (13.4%). While there is a need to acknowledge that these tools are still popular in certain settings and situations, the trend over the last five years has been downwards (see Figure 5). This year is no exception, with both tools noting a decline in usage since last year, of 2.3 and 2.5 percentage points, respectively. The use of satellite phones (11.9%) is also low — and has dropped by ten-percentage points in the last two years. However, it is likely that this means of communication is likely to increase over time as the technology matures, it is added as default to more communications devices, and organizations seek back-up communication solutions for downtime of VoIP networks. Indeed, many new mobile phone models now include satellite communication capability for use in emergencies, demonstrating its usage becoming mainstream.

Evolution of lesser-used tools to manage emergency communications 2020-2024

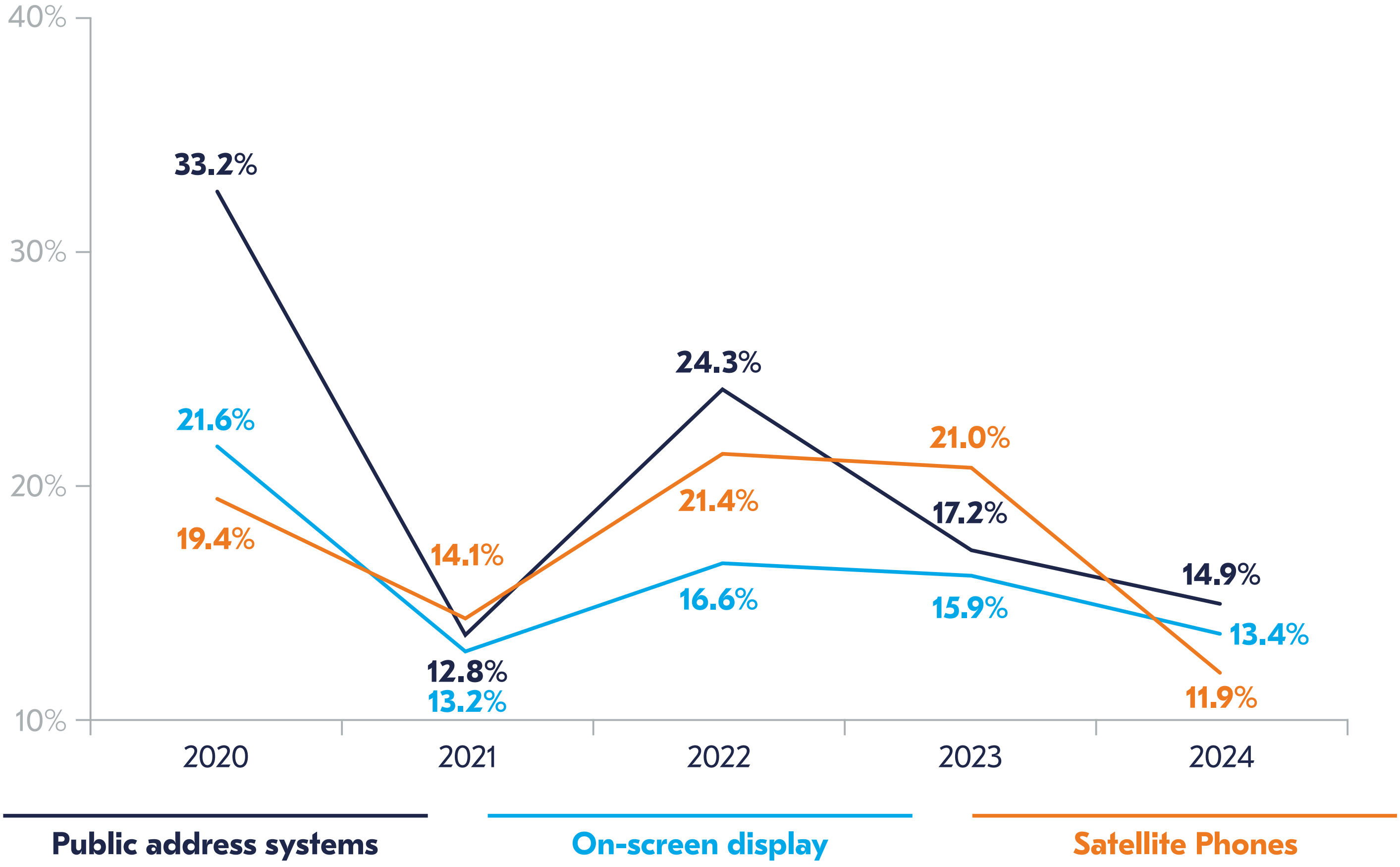


Figure 5. Evolution of lesser-used tools to manage emergency communications 2020-2024

Pagers are the least used emergency communication tool, present in only 4.5% of organizations (2023: 3.8%). This year it has seen a small increase in usage of 0.7 percentage points. While these devices may no longer be widely used, they continue to be important in specific, more niche sectors and/or particular circumstances. For instance, workers in healthcare and emergency services highlight the importance of these devices due to their durability and reliability. Nonetheless, there is a general acknowledgment that this type of tool is on the verge of becoming obsolete.

What devices are you using to manage emergency situations?

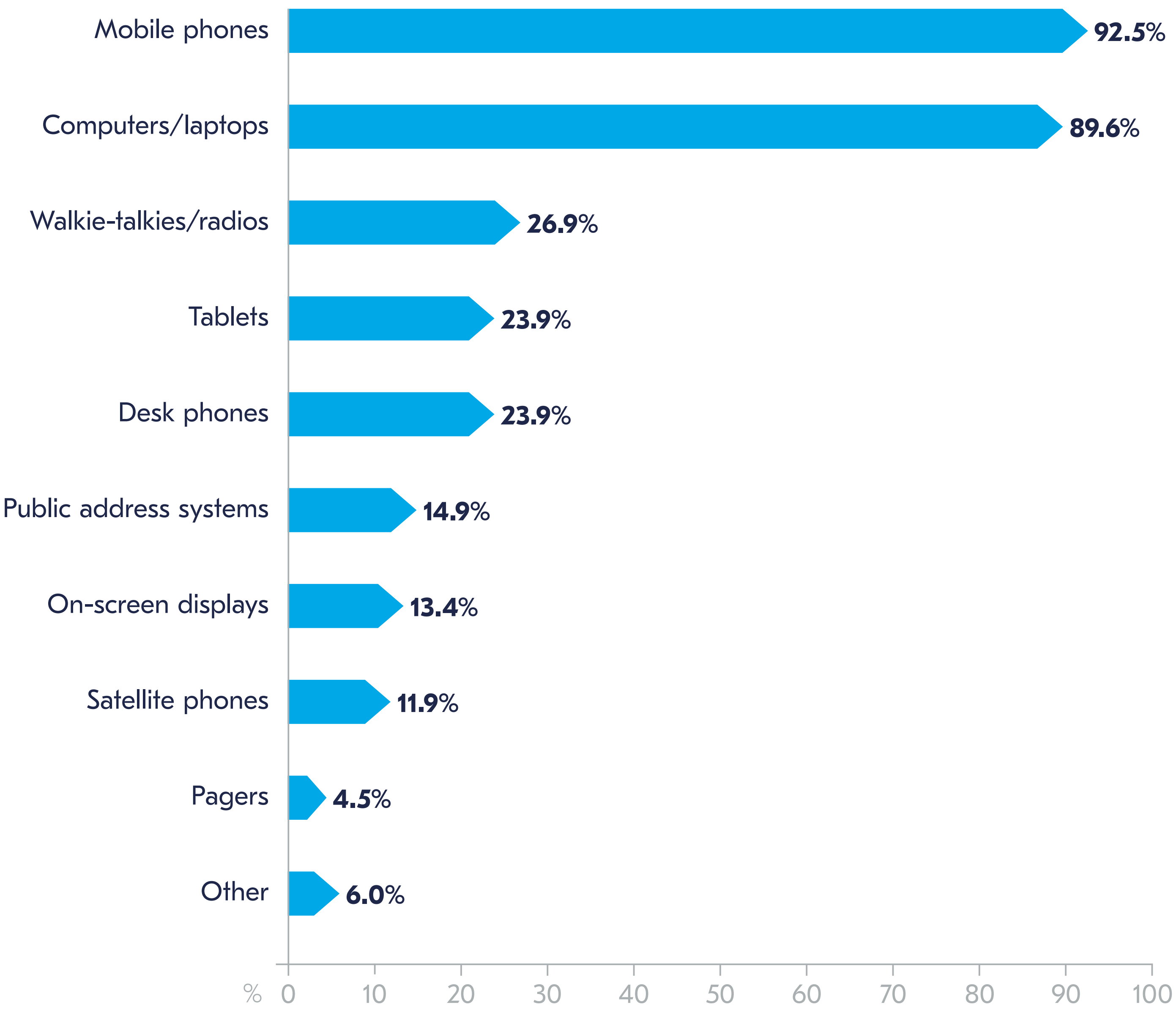


Figure 6. What devices are you using to manage emergency situations?

6% of respondents use other emergency devices, normally suitable to particular situations and/or circumstances. In this regard, an interviewee explained how they use duress alarms for their unique needs.

> **"We've just acquired a duress alarm system because we wanted to provide more safety to on-premises workers. We have outreach workers and sometimes they can be in high pressure situations, which could involve counselling. If we have face-to-face meetings and these emotional situations break out, the staff member could be in danger, hence the duress alarms."**
>
> Business continuity, charity sector, Australia

Many organizations are relying on Microsoft Teams for their emergency/crisis communications needs

More than a third of organizations are not yet using emergency communications software. Furthermore, the majority of surveyed organizations not using a tool are actually medium to large size companies (between 1,000-10,000 employees). However, the lack of a dedicated tool does not necessarily mean an organization is not using technology to manage crises, rather it indicates it is seeking alternative options to manage them. Demonstrating this is the fact that 95.6% of organizations that do not have a dedicated tool are either using incumbent software such as Microsoft Teams, are developing their own solutions, or are relying on other technology such as free messaging tools.

> **"The only real major problem that the organization had in the past has been COVID. It's a service driven operation and very phone/online based. If there was an emergency weather event, we could easily send everybody home and work on a phone. So the thinking often goes 'well, I've got a solution, I don't need a new one.' They have developed a few cloud-based response solutions, including Teams, and there is no perceived need for a new solution."**
>
> Business continuity, charity sector, Australia

> **"For slow-moving incidents or crises that allow more time for thoughtful communication, we will typically use more traditional communication platforms like corporate email, intranet, and Microsoft Teams."**
>
> Crisis management, insurance services, USA

Budgetary reasons are normally the primary reason for not using a dedicated tool (See Figure 8), but this year the option was selected by only 14.7% of respondents, relegating it to second position. The top reason cited this year is the successful adaptation of other tools (such as Microsoft Teams) to use in crisis situations. This suggests that while these organizations may not invest in a dedicated tool, they have at least identified the need for an emergency communications tool and no longer use lack of budget as a reason for not having one. As mentioned in the previous paragraph, some organizations choose enterprise technology such as Microsoft Teams as an emergency communication tool. However, while a powerful collaboration tool, consideration needs to be made to potential network, power, or platform downtime. This is of particular relevance in countries which have regular blackouts to reduce the strain on energy networks, such as South Africa. Consideration also needs to be made to ensure there is not an overreliance on a single platform.

> **"In relation to challenges within a crisis, there is a high reliance on Microsoft apps. I think it's very difficult to get other communications methods going if we are so invested in one provider; and that becomes a vulnerability."**
>
> Crisis management, insurance services, USA

> **"I think where everybody stumbles is around email and instant messages as it's not easy to do when Internet service is not available. You want to be able to do things through that corporate email box, especially if the impact is so big that you have got to make some sort of press statement."**
>
> Crisis management, financial services, USA

What is the main reason for you not having or not planning to have a tool/software for emergency communications/crisis management?

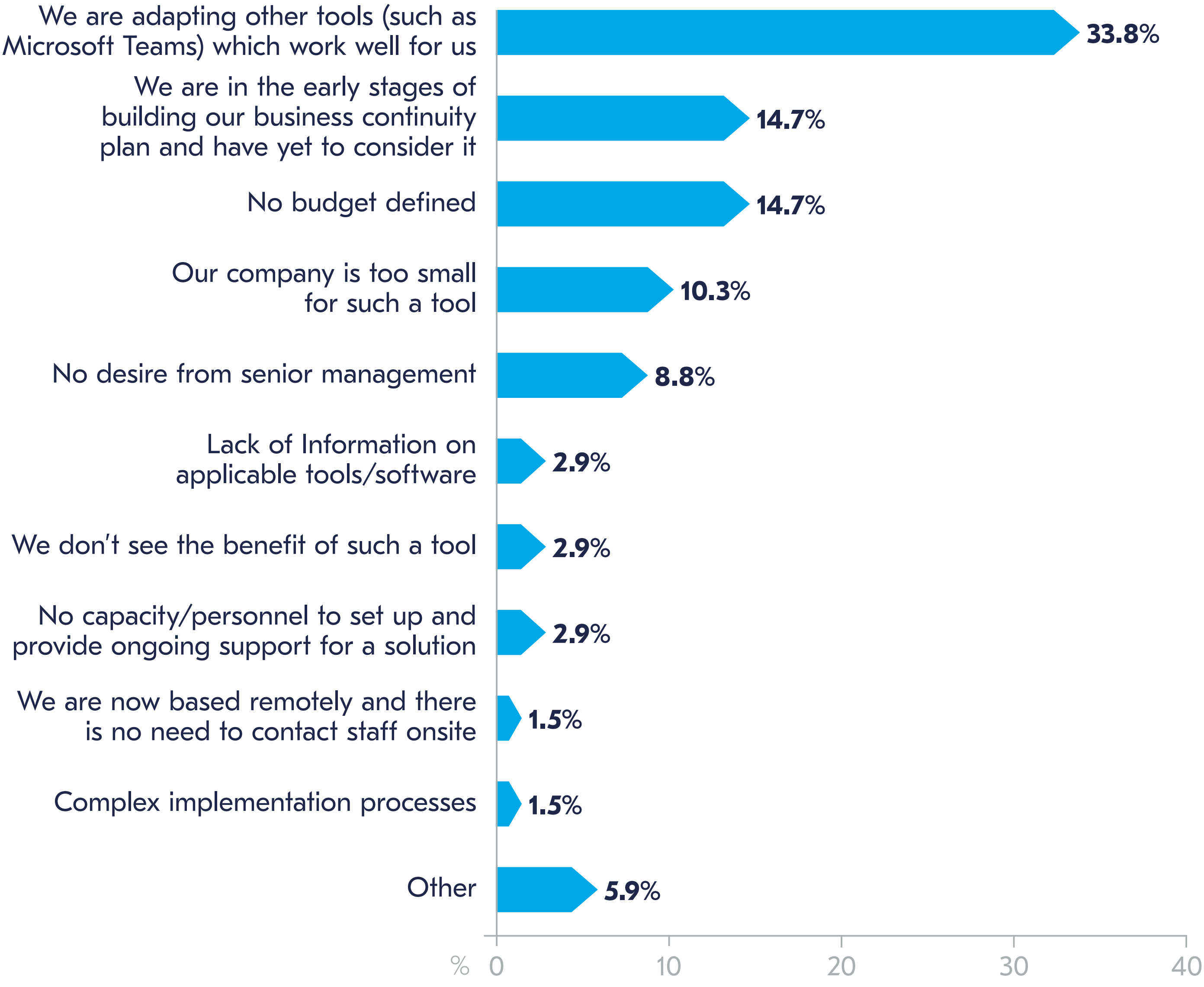


Figure 7. What is the main reason for you not having or not planning to have a tool/software for emergency communications/crisis management?

'No budget defined' as the reason for not having an emergency communication tool within organizations 2016-2024

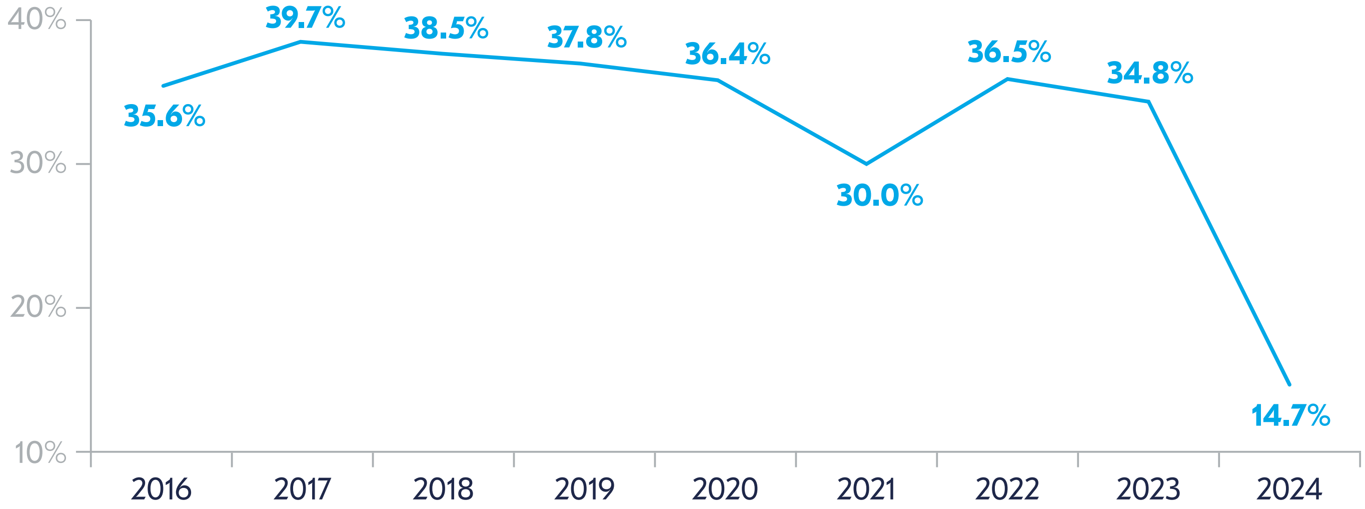


Figure 8. 'No budget defined' as the reason for not having an emergency communication tool within organizations 2016-2024

Other reasons given by respondents for not having an emergency communications tool in place are that business continuity is still in its infancy in their organization and they are not yet in a place to consider such a solution (14.7%); and believing that the organization is too small to need an emergency communications tool (10.3%), in third place. Interviewees also cited other reasons for using a specialist solution.

> **"When it comes to apps, what scares me is competition. You have to work through all the options and decide which one is best for you by sitting through many product demonstrations. I've got to interpret all those things and see how that is going to work within my organization. Then another issue is having to get all the tools we already have to integrate and talk to each other. That's really hard. Everything has its own language."**
>
> Business continuity, charity sector, Australia

> **"We don't have mass communication methods because the organization is so restricted on its IT capabilities. You couldn't put a broadcast out or anything like that in the settings I am familiar with."**
>
> Emergency planning manager, health sector, UK

Software-as-a-service is the norm – with organizations increasingly turning to hybrid options

Of those organizations using an emergency communications tool, 85.7% are using SaaS either as a pure SaaS solution (61.1%) or as a hybrid SaaS/installed solution (24.6%). In recent years, adoption of SaaS has grown steadily. With most organizations preferring software hosted in the cloud for easier management and its employability across multiple platforms, SaaS solutions have become the tool of choice.

It is important to note that 2024 is the first year that 'hybrid' has been included in the survey as an option, in order to account for the above scenario.

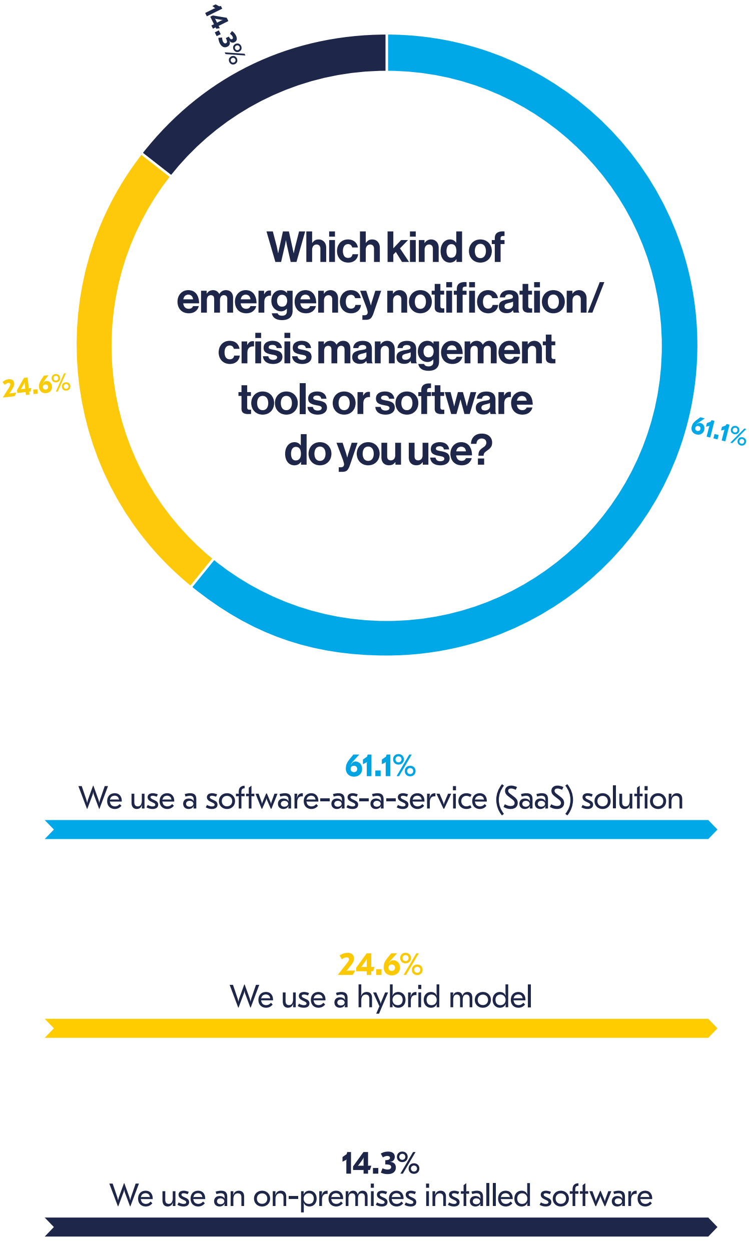


Figure 9. Which kind of emergency notification/crisis management tools or software do you use?

Usage of SaaS tools within emergency communications plans 2020-2024

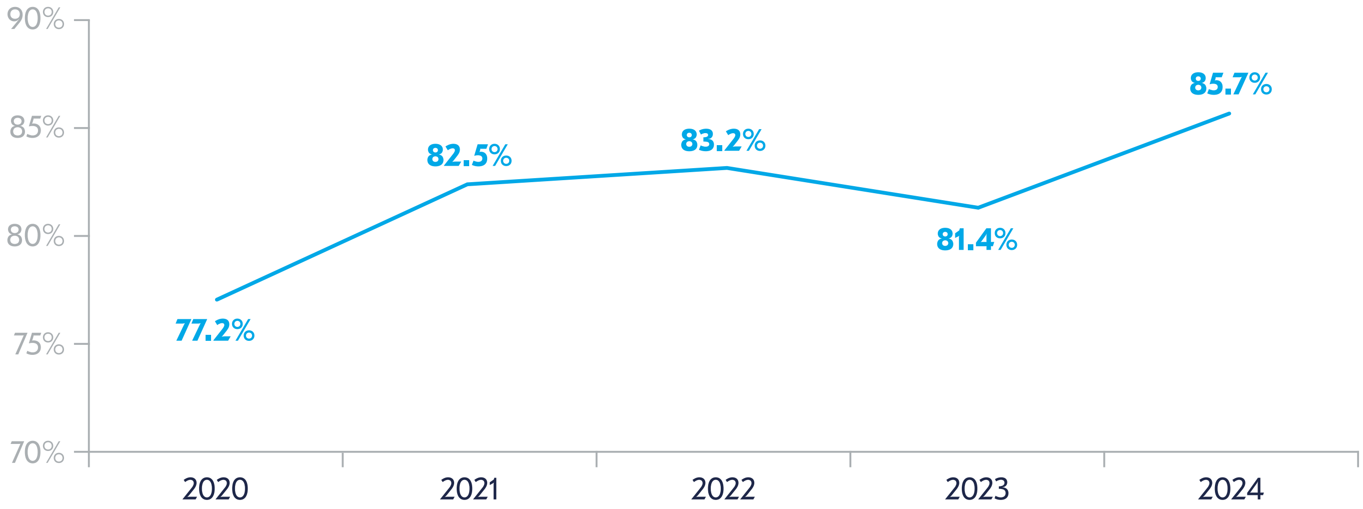
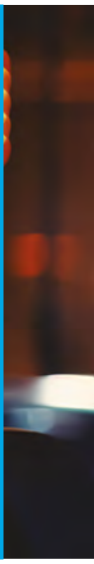


Figure 10. Usage of SaaS tools within emergency communications plans 2020-2024

Hybrid solutions offer a versatile and adaptive framework that allows organizations to benefit from the advantages of SaaS (e.g. multiplatform flexibility, speed, and reliability) but also use existing corporate systems as the backbone. This can help with integrating HR systems, for example, or enabling users to use familiar enterprise software with add-ons for use in emergency situations. It can also provide cost savings and efficiencies, depending on the existing incumbent software. Interviewees explained how they use a hybrid approach of communicating with different stakeholders in crisis situations.

> **"We use a notification software solution that we purchased for mass notifications. However, we also post paper copies because we have some workers that don't have their phones with them while working and some don't have a cell phone at all. Moreover, some of the older residents in our neighbourhood don't have computers. So, we'll have staff or firefighters go door-to-door to connect with people that are in high-risk areas."**
>
> Emergency management & business continuity, government administration, Canada

> **"We operate a hybrid response system. The interconnection between the two tools is managed manually. In this case, it is important that the structure is well-defined and tested. We spend a lot of time testing the system and if it's not efficient, we escalate."**
>
> Certification implementer, manufacturing sector, Italy



The use of installed software only remains in gradual decline. Just 14.3% of respondents chose this option, with usage tending to be reserved for sectors and regions where localised control is required, dated legacy systems are used, or there are significant data protection concerns. Usage is common in settings such as military operations, government, and emergency services as they tend to have their own, often government-mandated, solutions already in place.

Decline in the usage of on-premises installed software 2020-2024

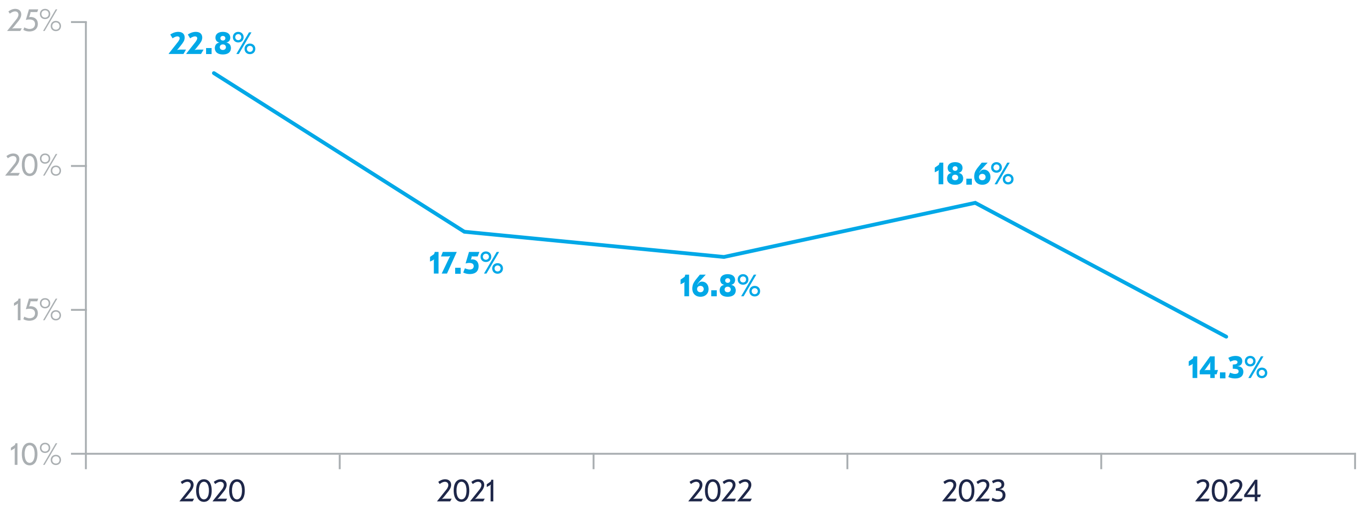


Figure 11. Decline in the usage of on-premises installed software 2020-2024

Alerting and mobilising a large number of people very quickly is still the primary use of emergency communication systems

Organizations use crisis communications systems in different ways, each having a unique set of 'must haves' and 'nice to haves'. However, over the last five years, the same four features have registered at the top of the list.

The need to alert and mobilise a large number of people extremely quickly remains the top requirement from organizations' emergency communications tools. 81.3% of respondents selected this option, slightly down on the previous year (2023: 85.9%). Given that the key priority in many crises is staff safety, it is not a surprise to see this option at the top of the list. Some organizations prefer to take a sequential approach to their response by transmitting vital information first and interactive collaboration second, ensuring a well-rounded and efficient response to crisis scenarios. As communications become more sophisticated however, some interviewees emphasised the increasing importance of having a two-way communication system from the start, with collaboration viewed as the starting point for a successful activation.

Crisis handling (e.g. real-time task management, reporting, status updates) is in second place with 43.3% of respondents selecting this option (2023: 46.1%). Reporting mechanisms can capture and disseminate information quickly (particularly now artificial intelligence (AI) is being increasingly deployed to assist with datamining and analysis), resulting in prompt and actionable information to assist with the crisis. Additionally, regular status updates provide the ability to communicate changes in the response, progress made, or new issues arising.

As in the BCI Emergency & Crisis Communications Report 2023, there is a significant concern over employee safety, especially for lone workers. With many organizations choosing hybrid working environments, the regularity of employees being alone in offices has decreased compared to pandemic times. According to the UK Office for National Statistics, after government COVID-19 guidance on working from home was lifted, the proportion of workers working under hybrid patterns had risen from 13% in early February 2022 to 24% in May 2022. At the same time, the percentage of the workforce working exclusively from home has fallen from 22% to 14% in the same period[9]. Moreover, the Commercial Observer reported that 40% of the worldwide workforce had returned to on-site work by the end of 2021.[10]

Consequently, as employers ask personnel to go back to on-premise or hybrid working patterns, employee safety is again recognised as an essential element in the emergency communication plans of many organizations, with 38.8% viewing this as a priority feature of their tool.

Enabling communication in teams is in fourth place this year, with just over a third of respondents selecting this option (34.3%). The importance of multi-way communications has already been highlighted in this report, but given most tools provide this as standard, such communication can serve as a vital link to knowing that an employee is safe. Such tools can also be vital for response teams on the ground to ensure that they can collaborate during the response process. Two-way communications can also provide an audit trail, which can be particularly useful in knowing if a message has been read (although options for this can be limited on free messaging solutions).

In which areas does your tool/software support you?

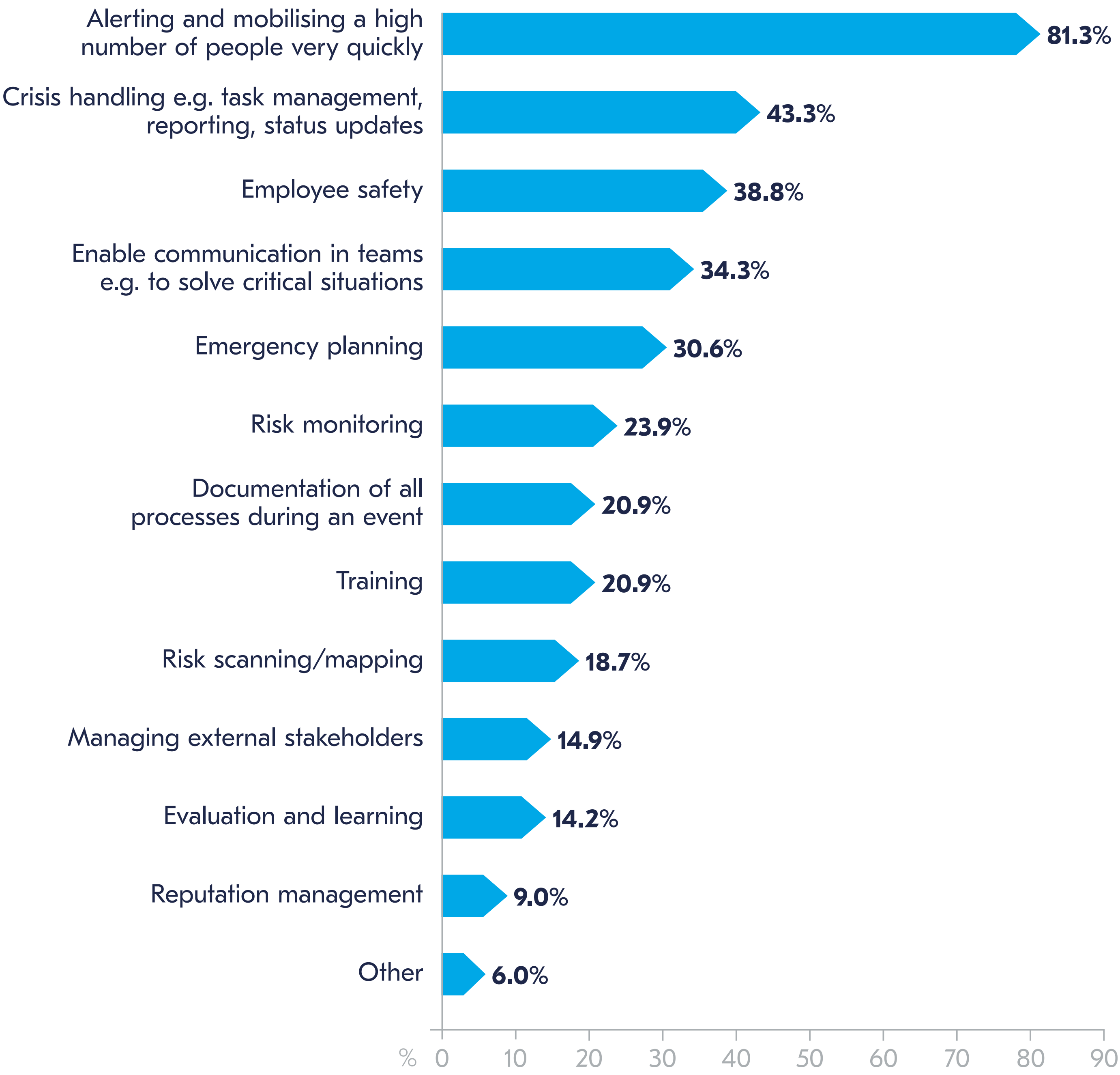


Figure 12. In which areas does your tool/software support you?

The least popular functions supported by crisis management tools are the managing of external stakeholders (which is frequently handled by PR and/or corporate communications) at 14.9%; evaluation and learning (14.2%); and reputation management (6%). Interviewees explained why certain tools had been selected for use in their organizations.

“The tool that we have in use is for threat monitoring. Because we are a hybrid organization, we monitor homes and offices for physical-based threats through this tool. These would include weather threats, protests, civil unrest, and aggressors.”

Crisis management,
insurance services, USA

“Having moved to a hybrid workforce model, being able to map threats geographically is much more important to us now, because we have to know what the specific threats are around our employees’ homes. Then we can plan to shift business if we need to.”

Crisis management,
insurance services, USA

“We have an automated notification system that has a mobile app that we encourage people to use. But it’s a bit difficult telling people to put apps on their own phones because of GDPR issues.”

Crisis management, financial services, USA

“Our tool has extensive reports that can tell us who the people are that we could not connect to and then we can find out why we couldn’t connect to them, so we can follow up on that. This way it helps us with the documentation of processes.”

Emergency management &
business continuity, government
administration, Canada

“We have some workers who work by themselves and our notification tool helps us keep them safe. If we have, for instance, an active threat happening in an area, then all staff - because we don’t know where they are exactly - will immediately get notified on their personal devices of the threat and the general location.”

Emergency management & business continuity,
government administration, Canada

Communication techniques during a crisis

For internal communication during a crisis, there is a growing emphasis on employing multiple solutions simultaneously in an effort to enhance redundancy and contingency within emergency communication plans. This is something which the research for previous BCI reports has also shown[11]. Consequently, the practice of incorporating a layered approach of overlapping tools and methods is increasingly becoming the norm. However, having multiple layers of tools within emergency response does not come without its challenges. Interviewees explained the positives and negatives of the layered approach.

> **"I think that before COVID-19, people used to try to have an emergency communications tool that could do everything. Not that it's easy to find. However, I think that, lately, we're seeing a lot of layering of tools, especially in organizations that actually don't have a budget. They use free tools but they layer them as well."**
>
> Crisis management, financial services, USA

> **"Having multiple channels of communications presents challenges for us because instead of having one consolidated information channel in order to notify people more quickly and efficiently, you need to support and control multiple channels at the same time."**
>
> CEO, professional services, Ukraine

The preferred method of communication for activating the crisis team is emergency communications management software (46.7%). As these tools are dedicated to use only within emergency scenarios, this ensures that messages are separated from the 'noise' of other corporate systems and notifications from other applications. They also provide encryption and meet certain security standards, ensuring that sensitive information is transmitted securely, as well as ensuring an audit trail of messages so those activating the system know if a message has been delivered or read. Typically, if a message is not received, an organization can then send out a secondary message through another platform. It should, of course, be emphasised that any organization taking on a new technology should ensure that the security standards and encryption meet the levels required by both themselves, their industry and, in some cases, their country.

Tools which have been developed in-house are the second most popular way of activating the crisis team, at 40.7%. Although some organizations have developed bespoke internal software, some interviewees spoke how they had defined 'in-house developed tools' as using advanced options on Microsoft Teams, or using add-on products for the platform.

Dedicated crisis telephone lines are in third place (35.7%) and secure messaging apps are the fourth most popular (28.7%). Fifth place is taken by the long-established tool of call trees (28.1%). The use of call trees, while limited in features and potentially giving rise to coordination and scalability challenges, can provide an effective communication back-up if Internet services are down. However, the limited features for coordination and scalability challenges of manual call trees may impede their effectiveness, particularly as the crisis team size increases. Nonetheless, call trees have moved on from the traditional cascade effect where an initial call would be made to limited individuals, who would then pass the message on to more individuals, who would then pass on to more – until the whole organization was contacted (if needed). Call trees now tend to be an automated solution where human intervention is limited and are typically added as a feature of emergency and crisis communication solutions.

Free messaging apps occupy a lowly position in the table (26.9%). Although this report has discussed the pitfalls of using free messaging apps, it should be noted that some free apps are now offering enhanced business messaging services as paid-for solutions (such as WhatsApp Business). However, products should still be evaluated before they are employed as many of these business solutions' features are around enhancing sales performance and customer experience rather than providing a workable solution for emergency communication[12].

Still, nearly six in ten organizations are using free applications to some extent and the perception of these is mixed amongst interviewees.

> **"I can reach stakeholders via free messaging tools directly. I also have communication with my customers through messenger applications. This works well as you get messages out more quickly than with corporate emails, for example."**
>
> CEO, professional services, Ukraine

> **"Here in Ukraine, we widely use Viber as a messaging app, or Telegram. However Viber is not used within the international community. The global environment uses WhatsApp and Signal, making this process more complex and more time consuming."**
>
> CEO, professional services, Ukraine

> **"In Indonesia we have a huge site with more than 3,000 people. There is a high turnover in the workforce with many employees on short fixed-term contracts as well as the use of subcontractors for internal processes. So the company has some difficulty mapping all of these people and third-parties. In that site there is daily use of WhatsApp. It's easier for them to promote this kind of team communication tool."**
>
> Certification implementer, manufacturing sector, Italy

> **"We do have associates outside of the US and WhatsApp is a much-preferred method of communicating with them. We are investigating WhatsApp integration with our vendor. However, secure communications would not be sent out via WhatsApp."**
>
> Crisis management, insurance services, USA

> **"There is this cultural gap in the usage of free tools like WhatsApp. In some countries where there aren't restrictive privacy laws, they can use specific emergency communication tools without issues. But when there are some data privacy restrictions, they prefer to use something that is more user friendly but less safe. For example, if the company asks people: 'Can we use your private contact for emergency communication?' they are likely to respond 'no'. But if there is a WhatsApp group for the data team, they say 'Okay, can you invite me?' It's cultural."**
>
> Certification implementer, manufacturing sector, Italy

What methods of communication do you use to activate the crisis team?

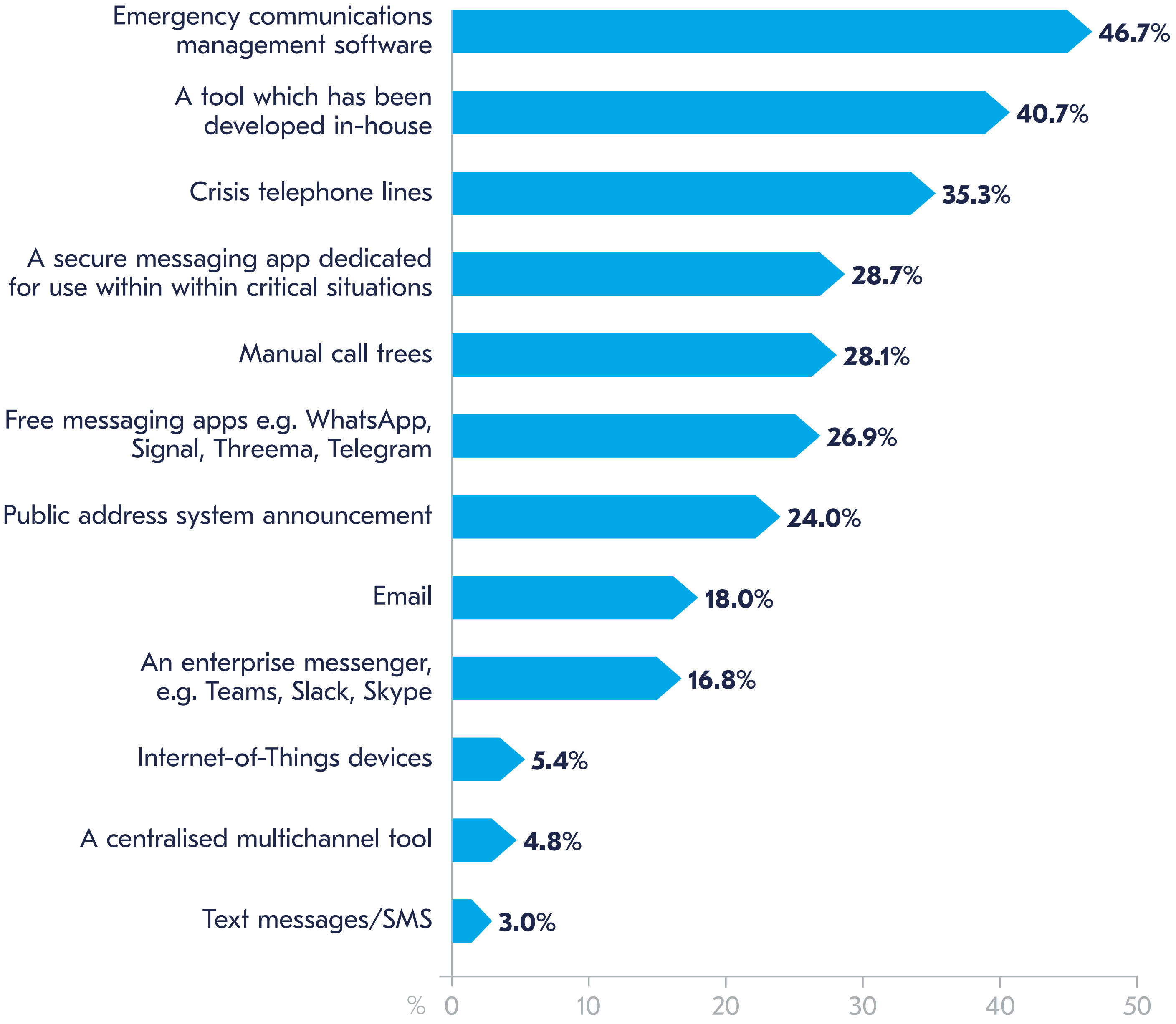


Figure 13. What methods of communication do you use to activate the crisis team?

Respondents were also asked how communications are carried out within the crisis team and, here, 59.9% of organizations selected an enterprise messenger such as Teams. This is a significant uptick from 2020 where 41.4% of settings used this kind of tool. The COVID-19 pandemic and the shift to remote working propelled enterprise messaging to become the primary communications medium in organizations and using its functionalities to communicate with others in a crisis team would be a natural step for many.

Email was the second-placed option this year (50.3% of respondents). While this is not necessarily the most effective way to activate the team or notify staff of an emergency situation, it would be effective to use this in the response phase of a crisis, particularly for sending messages and documents that are not time-critical.

Text messages were in third place, and still used by over a third of teams (34.1%). While many have switched to other methods for text-based communication (such as WhatsApp), a message sent via short message service (SMS) can still be transmitted in areas of low or weak network coverage.

Free messaging apps were the fourth most popular tool for communication in the crisis team (32.9%). While the issues with this method have already been highlighted in this section, for more casual communications within the team, free messaging apps can have their place as they can differentiate between casual communication in a crisis (e.g. messages to enquire about wellbeing, or details of a coffee shop where the crisis team is mustering) and critical messages (e.g. informing the team about a crucial new development in a crisis). However, in order to be effective, the team needs to be made aware of the different usages for each tool. The BCI Emergency & Crisis Communication Report 2023[13] noted the increased use of this type of tool within crisis response.

In fifth place, just over a quarter of respondents (26.9%) report using a dedicated secure messaging app. As mentioned previously, the centralised control provided by these platforms can help to streamline coordination efforts, enabling effective communication and collaboration among team members and they can also be the differentiator between critical messages and more casual communications. Dedicated messaging apps can also provide high levels of security, with functionality such as screenshot disabling and encryption of messages.

What methods of communications do you use to communicate within the crisis management team?

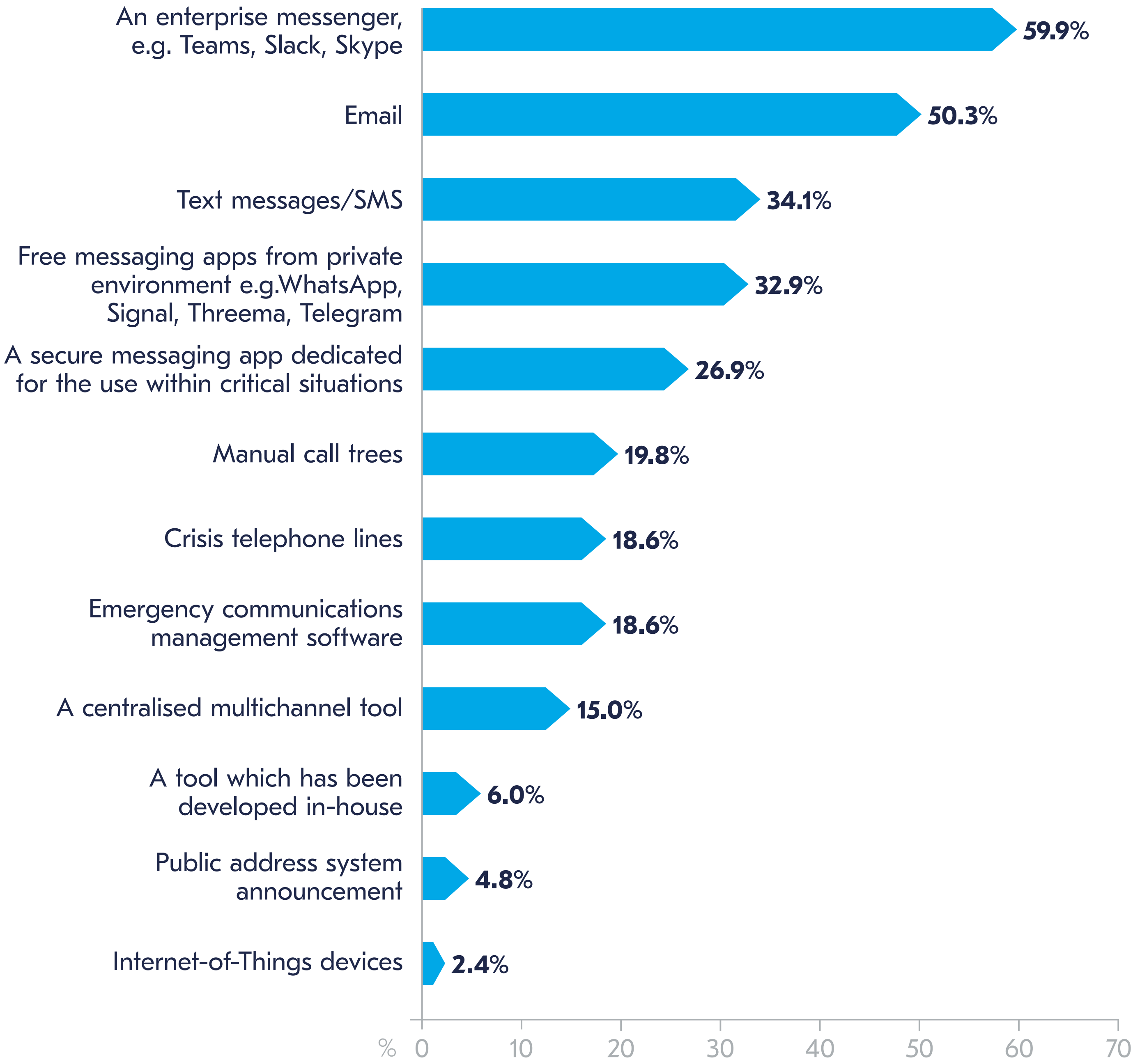


Figure 14. What methods of communications do you use to communicate within the crisis management team?

When communicating with the wider organization, the preferred method of communication remains email (59.9%). While this may not be the tool to communicate an urgent crisis, or may not even be possible during a cyber attack, for example, it can provide a means of getting a curated message out to staff about a crisis — particularly one which is ongoing. Some organizations have proforma messages created for different incidents which can be immediately sent out in the event of an emergency. However, interviewees discussed how they tended to use a layered approach to contact the wider organization through a mixture of email, messaging solutions, and, where appropriate, on-site communication tools.

What methods of communications do you use to communicate with the wider organization in a crisis?

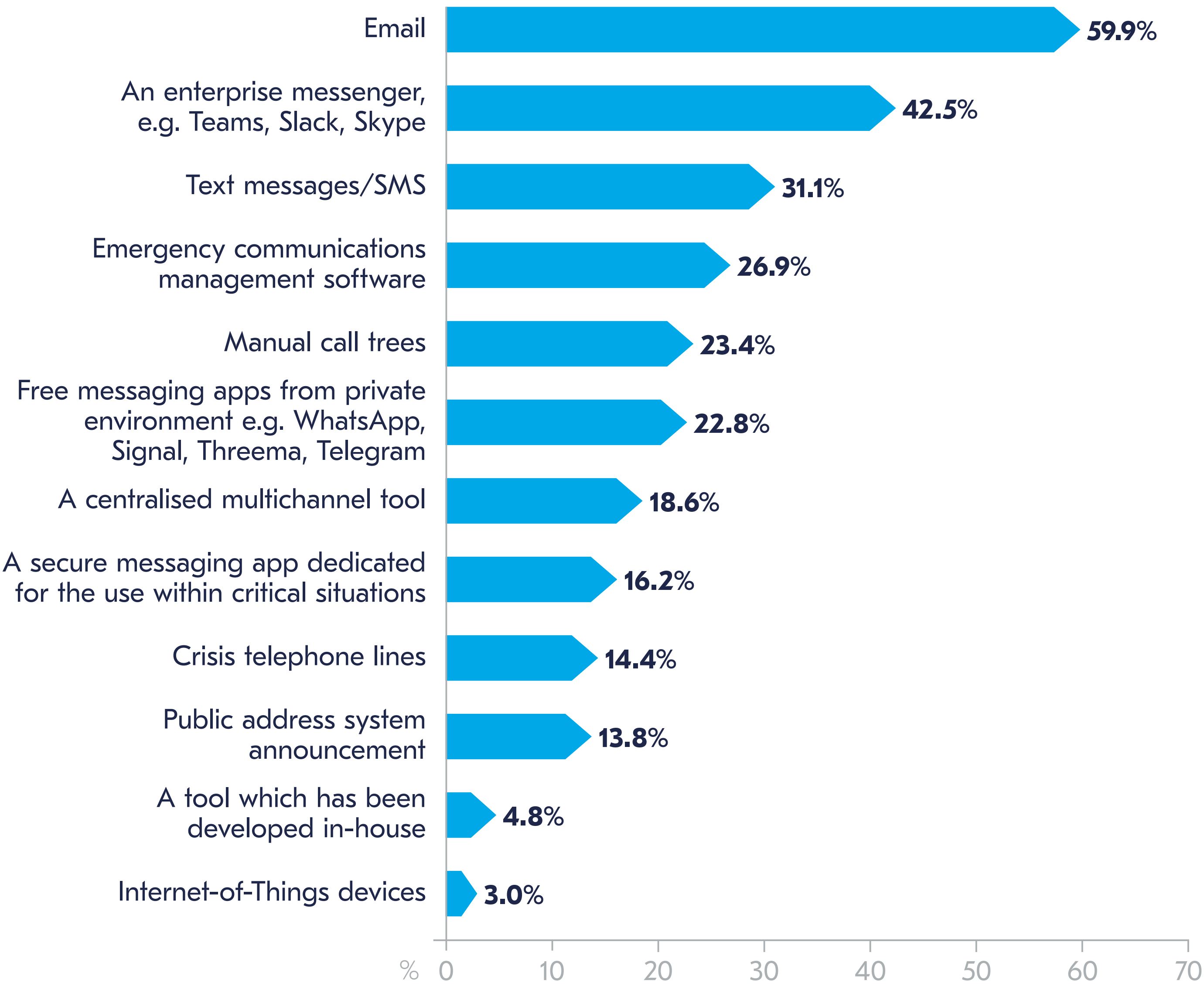


Figure 15. What methods of communications do you use to communicate with the wider organization in a crisis?

There is a record level of unhappiness with current emergency communications solutions

The optimal communication solution within emergency and crisis situations varies from one organization to another, a notion emphasised when participants were asked about their satisfaction levels with the tool they are currently using. Overall, most organizations are satisfied with their solution, with nearly 80% acknowledging their satisfaction with their selected tool. The majority qualified their positive response with 'somewhat happy' (49.1%), and the remaining unequivocally happy (30.7%).

However, the 20.3% who indicated dissatisfaction, although a minority, constitute a segment that is starting to grow substantially (2023: 16.2%). Indeed, the 2024 report records the highest dissatisfaction levels ever among respondents, reflecting the heightened expectations placed on tools. However, the dissatisfaction does differ according to the type of tool used: those organizations using on-premises solutions are the most dissatisfied (20.0%), followed by organizations using a hybrid solution for their emergency response (15%). Those using a pure SaaS solution record the highest level of satisfaction, with only 4.9% of SaaS users reporting they are unhappy with their solution.

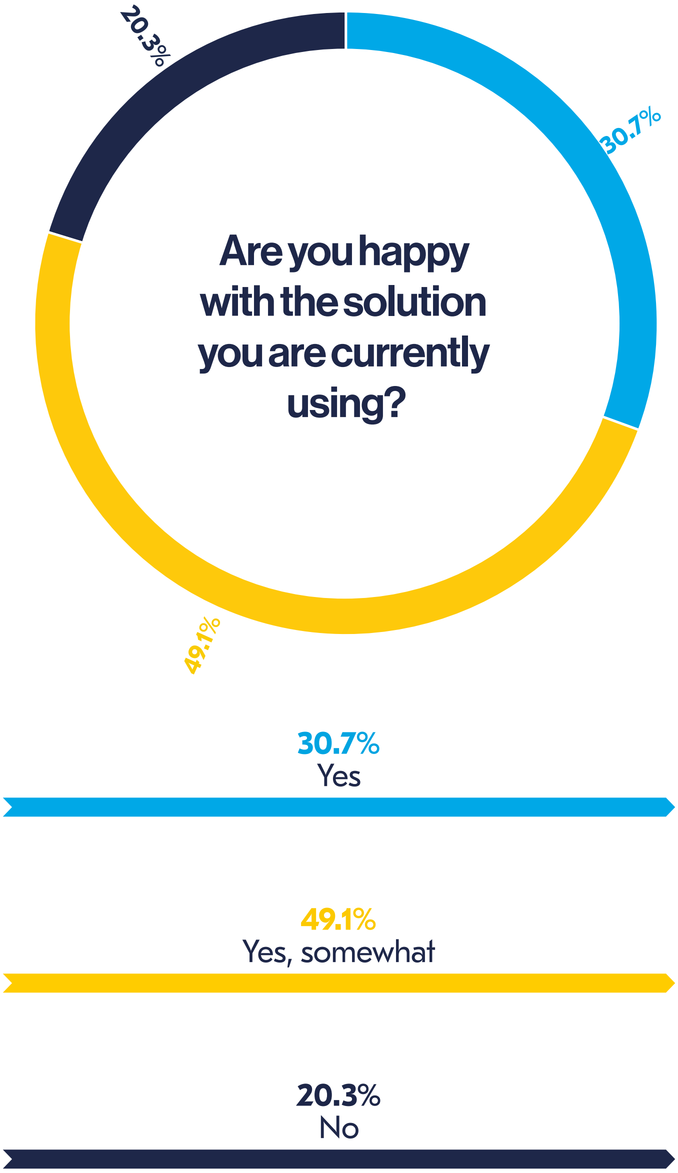


Figure 16. Are you happy with the solution you are currently using?

Levels of satisfaction also vary according to the communication method used during emergencies: 63.6% of respondents who do not use any dedicated emergency notification/crisis management tools or software are unhappy with the solution they are leveraging. Moreover, the discontent with the tools being used is indicative of a growing reliance on less sophisticated tools, often chosen for their cost-effectiveness, such as enterprise software and free messaging apps. When analysing those respondents who are not happy with their current solution, 83.3% use free messaging apps to communicate within their crisis team and 79.2% use an enterprise messenger. Just 38.5% of those using a dedicated messaging app report not being happy with the solution.

Percentage of respondents reporting unhappiness with their current emergency communication solution 2021-2024

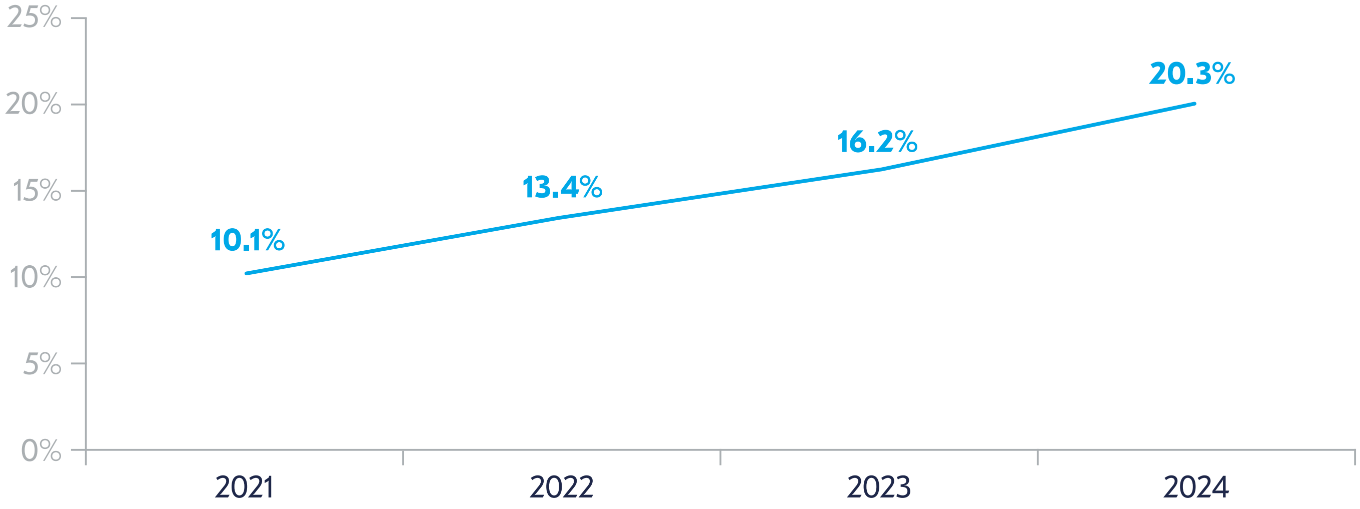


Figure 17. Are you happy with the solution you are currently using? Percentage of respondents answering 'no'.

When respondents were asked about the reasons for their dissatisfaction with their tool, the same three factors that have been at the top of the list for the past five years were again selected this year: the need for better integration with alerting scenarios (48.3%), lack of functionality (31.6%), and not being able to afford their ideal solution (19.3%). Legacy issues also feature as a top concern for 17.5% of organizations, increasing 7.6 percentage points since the 2023 report. One interviewee explained that their organization's tool was not user-friendly, while another explained the problem of legacy systems.

"It's not easy to manage the specific tools that we use. When we approach dedicated tooling, we experience some challenges due to the fact that the tool is not user-friendly and has a certain protocol that needs to be followed."

Certification implementer,
manufacturing sector, Italy

"Our organization has got lots of legacy systems. We are not able to start again with new systems because of the huge funding issue in bringing this technology in. We therefore tend to build on what we've got, which isn't ideal, and then we lack functionality which means we can't do that whole system communication."

Emergency planning manager,
health sector, UK

A respondent described how cost cutting meant their organization now used different tools across the organization and pointed to reduced effectiveness of their communication strategy: "Due to cost cutting exercises, the solution has become a disparate compilation of different standalone tools rather than a seamless all-in-one solution." Meanwhile, another respondent highlighted issues with user rights with the app only allowing the most senior staff to manage the solution: "The current solution is managed by our top tier government, giving us limited administrative rights which is challenging when designing messaging."

Several other survey participants also highlighted organizational problems around tool utilisation, with one saying that: "The lack of a formalised and adopted procedure throughout leaves the effectiveness of the communication dependant on the few people involved in operating the tool." Another respondent explained that: "Their company-wide process is undefined or non-existent."

Reasons for respondents being only 'somewhat happy' or 'not happy' with their current emergency communications tool

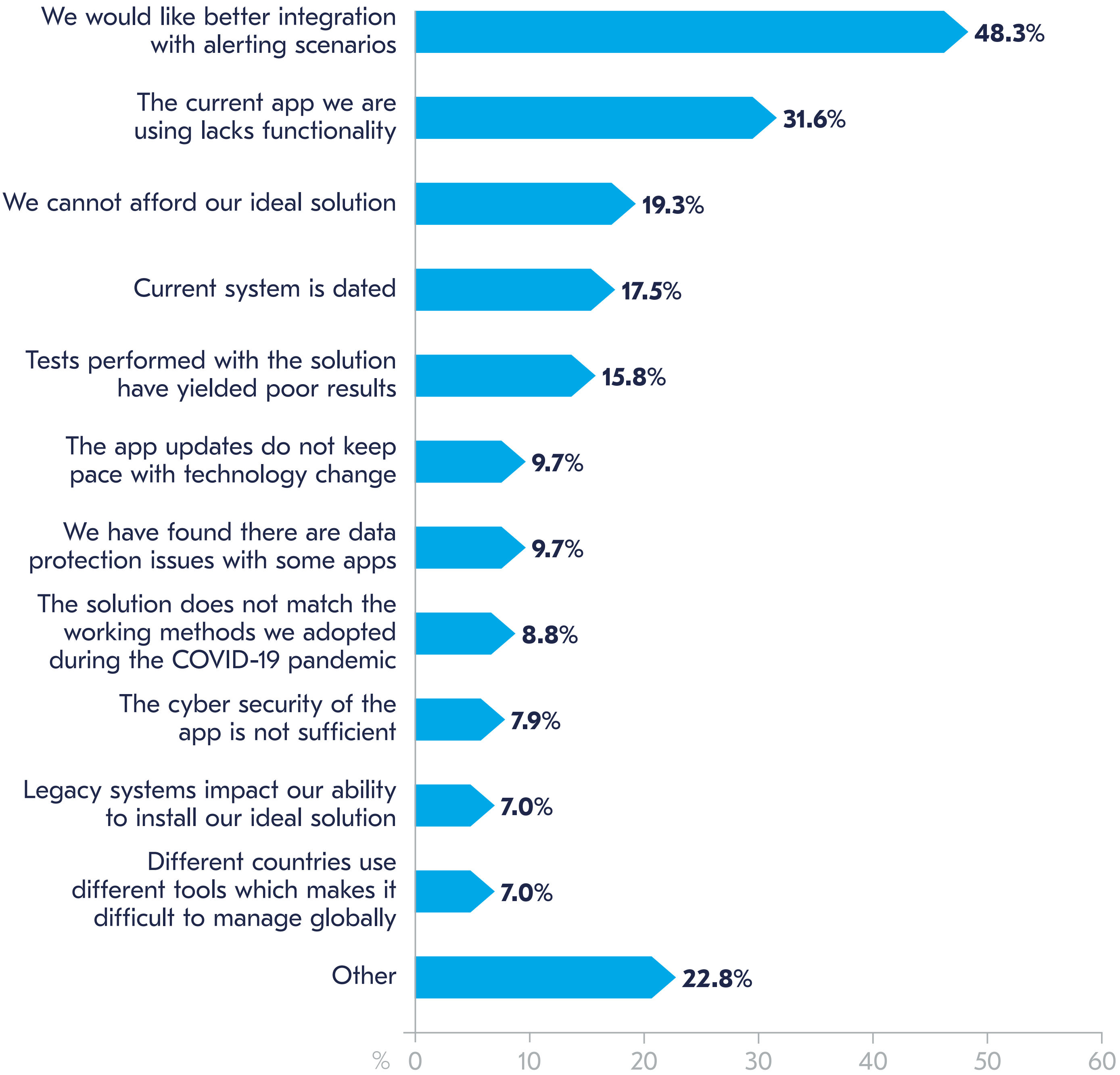


Figure 18. Reasons for respondents being only 'somewhat happy' or 'not happy' with their current emergency communications tool

2 Tool requirements

Tool requirements

- Collaborative functionality is the most requested feature by practitioners in their emergency communications solutions.
- The shift in views on alerting and emergency communication tools in the past two years emphasises the growing role of technology and the growing awareness of the importance of ensuring that communication can continue if an outage occurs.
- Organizations are becoming more aware of the dependency of their emergency and crisis communications plans on network service and are seeking workaround solutions.
- Organizations are starting to consider how AI can be used in their emergency and crisis communications programmes.

Survey respondents were asked to rate 12 features of emergency communications tools to determine their significance. The functionalities most valued by respondents revolve around collaborative work, perhaps not surprising given the increased emphasis on building effective virtual collaboration since the COVID-19 pandemic years[14].

Respondents' top four functionality features in emergency communications tools (percentage of respondents answering 'critical' or 'very important')

1 **80.9%**
Enable expert teams to collaborate easily and in real-time

2 **79.2%**
Effective communication with remote teams

3 **76.5%**
Constant exchange of information to enable decision-making

4 **72.5%**
One-way (mass) communication

Recognising the need for collaboration, respondents emphasised that technology should facilitate easy real-time collaboration among expert teams, enabling not only the effective communication with remote teams, but also the constant exchange of information crucial for decision-making. Over three-quarters of respondents considered these collaborative features as 'critical' or 'very important' for their organizations.

Interestingly, one-way mass communication, which was the top choice in the 2023 report, now ranks fourth in practitioners' considerations, with 37.9% saying it was of critical importance in emergency communication plans. This demonstrates the multi-layered approach that organizations are more frequently employing to ensure that all employees are effectively notified.

The increasing preference for collaborative tools in crisis situations does, however, underscore the ongoing significance of working collectively when faced with emergencies. Whether collaborating with experts, colleagues, or top management, the ability to work together remains crucial for a coordinated, cross-departmental response. A collaborative approach also means that staff at all levels feel engaged during an emergency and will feel incentivised to ensure that they follow procedures and protocols, as well as to input valuable information where required.

How important are the following aspects for your alerting and emergency communications?

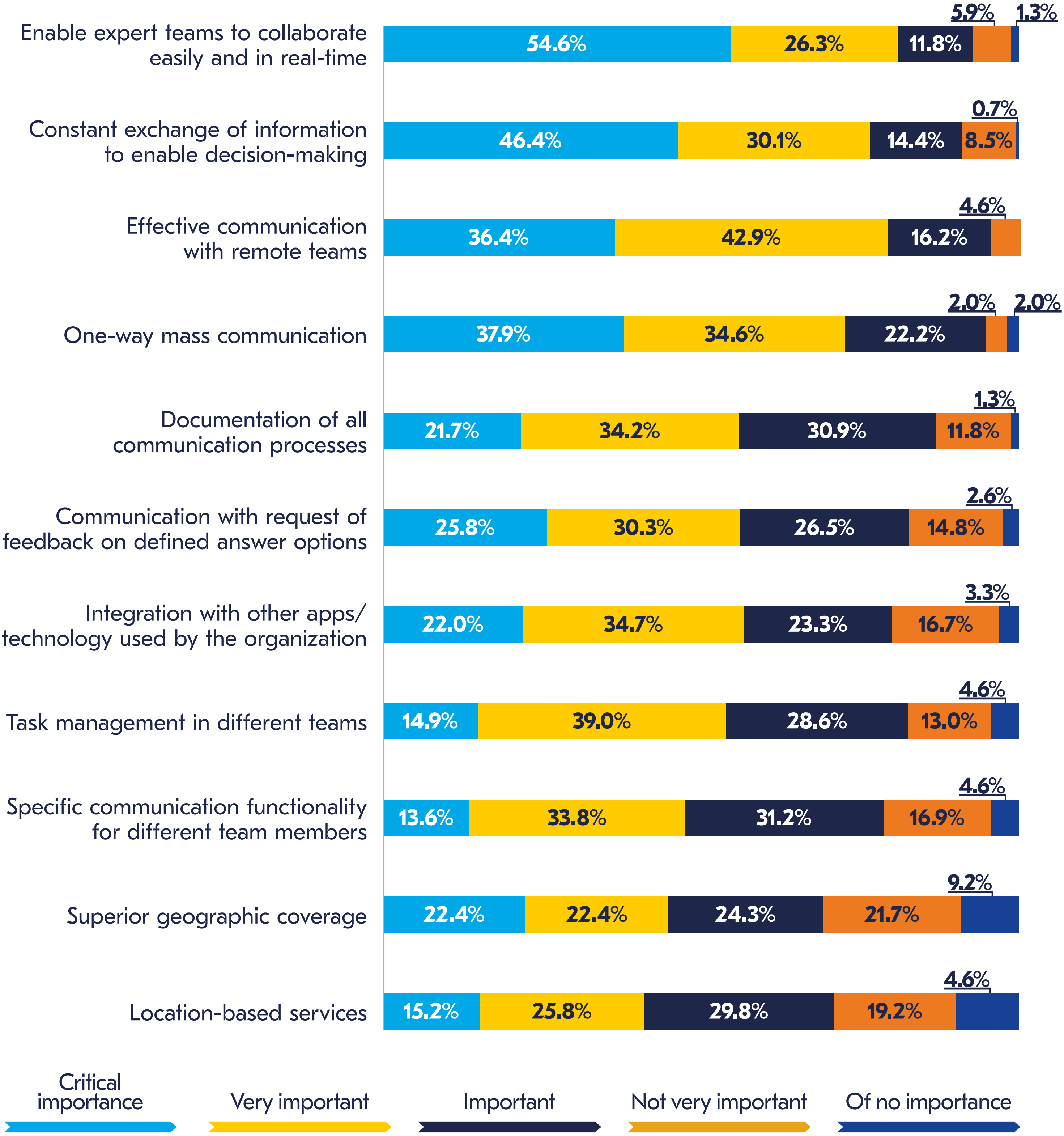


Figure 19. How important are the following aspects for your alerting and emergency communications? (Scale 1-5)

Other ‘critical’ and ‘very important’ aspects of emergency communication tools selected by respondents are integration with existing apps/technology used within organizations (56.7%), two-way communication (56.1%), and documentation of communication processes (55.9%).

These figures were supported when respondents were asked to clarify how their alerting and emergency communications tools/systems had changed over the past two years. Frequent comments from survey respondents circled around the increasing importance of the role of technology and the criticality of communication within teams.

“The need for communicating with remote teams increased, and integration became more critical.”

“Messenger apps, installed on smartphones, now have a bigger role.”

“[Emergency communications] is more important than ever in terms of tech improvements, but also identifying the limitations of legacy emergency comms systems which can force teams to work in set ways without flexibility.”

“Rollout of digitisation of the phone network has focussed the mind on improving access to other resilient comms (satellite and radio comms). We are also looking into integrated business continuity management packages.”

“Our view has changed significantly, with bushfire and severe weather events being at the forefront of our planning. We are entering a severe weather season and we need to be able to contact and locate our staff and vice versa, especially for regional sites that are within bushfire, flood, and cyclone zones.”

“Microsoft Teams has changed a lot of our thinking. Now it is more critical to have activation and immediate online capabilities.”

Also, the incorporation of AI within emergency and crisis response is now something that professionals are starting to consider. In this light, a survey respondent commented that: “AI and how to manage AI effectively is becoming increasingly evident. We do not want to be left behind but are cautious about its adoption.” Interviewees also discussed the role of AI within crisis management settings.

"Nowadays I see data everywhere, but I don't see information. There's a difference. You can have data but who's turning it into actionable intelligence? Where is it being stored and is it accessible so it can become information for somebody to use? You need to elevate data into information. AI can help with data processing. AI can go through thousands of documents in a moment and categorise it. So that data now becomes usable information, key in emergency situations."

Business continuity, charity sector, Australia

"I have started to consider using artificial intelligence to create some messages for content management. For typical tasks it gives more productivity. However, for changes and for complex issues, it is not as good."

CEO, professional services, Ukraine

Survey respondents and interviewees also discussed the importance of ensuring that communications could still be made in the absence of network availability, as well as the increasing dependence of emergency services on having network and/or Internet connectivity. Indeed, one survey respondent commented that: "the question of out-of-band communications, i.e. what happens when all your systems are down, has become more important," while another said: "The ability to connect with employees when there is a technological interruption has become more important; and the ability to have GPS specific communication would be a real benefit."

An interviewee from Australia described a recent experience with network outages, highlighting the importance of having a back-up plan in place. Other interviewees also highlighted concerns about network coverage, as well as how customers are shaping some of the choices that organizations make in terms of emergency response.

"The event that happened today was with phones, the Internet, and pretty much everything linked to a certain provider being out. This was countrywide. Some train systems went down, some health systems went down, some banking systems went down. It was pretty heavy across the country. At work we weren't affected by it. We were on the alternative provider. If we weren't, what would we do? We do have pretty much everything on the cloud: our phone systems, our document management system, everything. The impact would have been considerable."

Business continuity, charity sector, Australia

“An important issue that we found with our alerting and response tools is the lack of service. Unless we’ve got really good signal, often the emergency tools fail. You’ve got black spots even within the hospital sites, where you can’t get a text message out. Unless we invest in capability and aerials from network providers on our sites, then it becomes really challenging.”

Emergency planning manager,
health sector, UK

“In case of a major power outage, historically that wouldn’t have been an issue if we were all in the office because we have a lot more redundancy built around our offices. However, it does become one where we have a large number of employees in their homes as we do now. However, no organization that I know of with the size of ours or larger can afford to build that same redundancy into the home of every single employee. In today’s hybrid workforce, knowing the threats and being able to pivot quickly when we have an incident has become much more important.”

Crisis management, insurance services, USA

“Nowadays out-of-band communications are crucial. When your normal communication methods are down, you need to make sure that you’ve still got different methods to get in contact with people.”

Crisis management,
financial services, USA

“I think that the big change we are seeing within the sector is the importance of the corporate crisis response. What we’ve done this year is made sure that we’ve got a detailed response put together quickly to respond to geopolitical or market-related pieces. Clients now are demanding information about events, wanting to check information, and at a high speed. Our organization is being pushed to respond to client questions on more market-affecting issues or even geopolitical issues as well.”

Crisis management,
financial services, USA

3

Activation of plans: triggers, response levels, and timing

Activation of plans: triggers, response levels, and timing

- The concept of the 'golden hour' for incident response persists, although most organizations are able to activate their plans much more quickly.
- The effectiveness of the response is influenced by the type of tool being leveraged in the crisis response.
- Organizations are activating plans more frequently than in the past.
- Expected response levels are particularly low, although this is more down to organizations putting tougher targets on their response times.
- The human factor remains the main barrier to higher response rates.

A quarter (25.5%) of respondents indicate that they did not need to activate their crisis management plans at all in 2023, a modest increase from the 21.0% reported in the previous report. While the non-activation of plans might be perceived positively by management, it emphasises the ongoing need for consistent testing and training to ensure organizational preparedness for future activations. However, there has been a five percentage-point increase in the number of organizations who have activated their emergency communications plans this year compared to the 2023 edition of this report. Nearly 65% of organizations (2023: 60.0%) had to activate their plans between one and five times in the last year. This rise may be attributed not only to the prevalence of hybrid working and some organizations returning entirely to on-site environments in 2023, but also the increasing number of incidents that organizations are reporting each year, as evidenced in the BCI Horizon Scan Report 2023[15].

Those having to activate a large number of times has diminished slightly from last year: only 4.8% had to execute their emergency communication plans 6-10 times (2023: 7.6%), while only 2.1% triggered their plans between 11 and 20 times in the same period (compared to 7.1% in 2023).

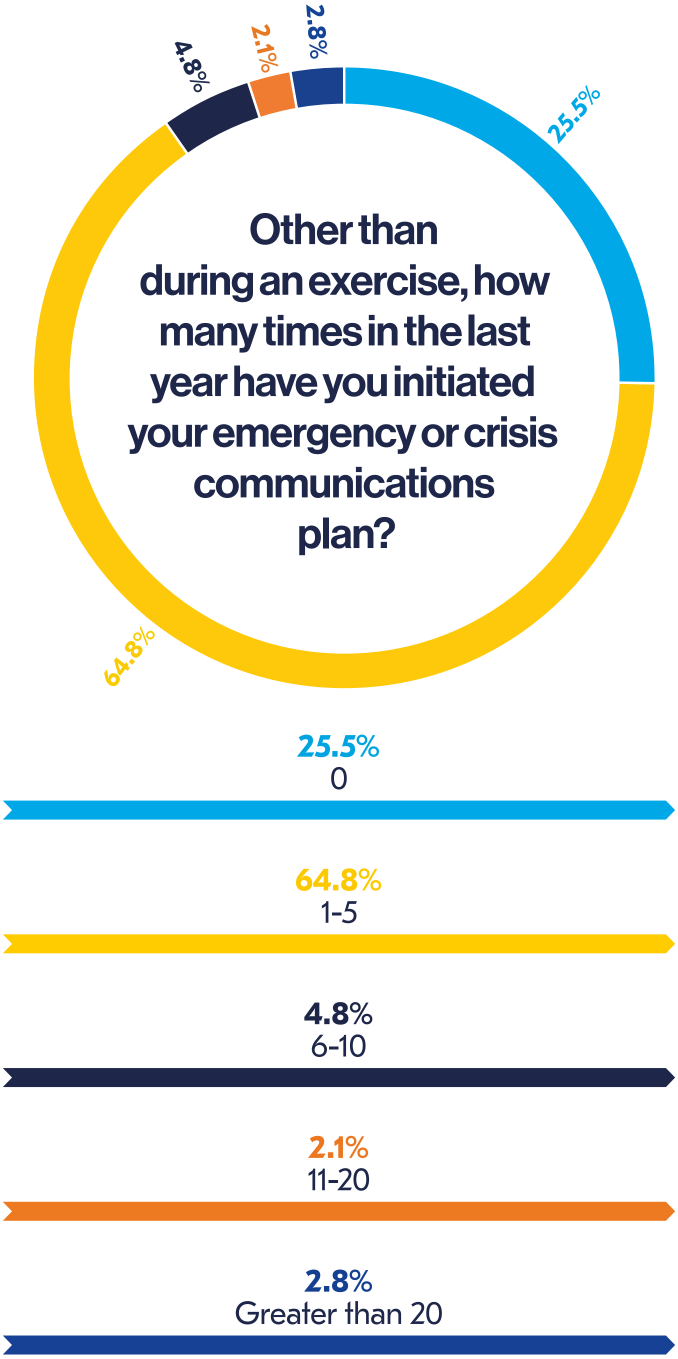


Figure 20. Other than during an exercise, how many times in the last year have you initiated your emergency or crisis communications plan?

Despite the year-on-year rise in the number of organizations not activating their plans at all, the percentage has fallen significantly over the past 10 years from 40.3% to 25.5% (CAGR: -4.5%). Furthermore, there has been a steady rise in the number of organizations requiring activation of their crisis plans between one and five times a year.

Activation of emergency communication plan in organizations 2015-2024

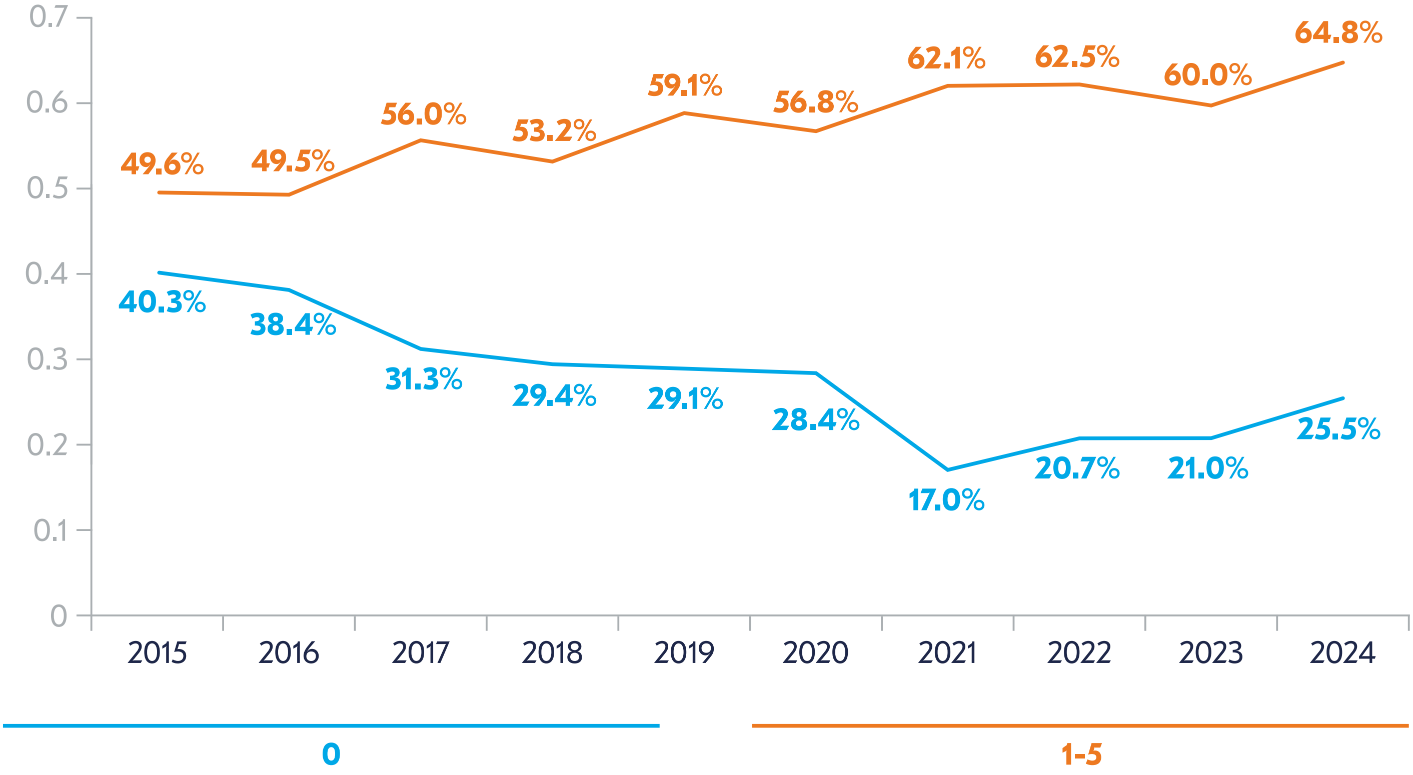


Figure 21. Activation of emergency communication plan in organizations 2015-2024

48.3% of emergency communication plan activations last year were due to extreme weather events. Weather-related incidents have consistently served as the primary catalyst for the activation of plans over the last decade, but with heightened frequency and seriousness of weather-related events as a result of the changing climate, it is anticipated that this pattern will persist (as highlighted by the BCI Severe Weather and Climate Risk Report 2023[16]).

"Last year there was a weather system that brought smoke from the northern fires as far down as New York, which caused poor air quality in the municipality. This was a new situation for us."

Emergency management & business continuity, government administration, Canada

"We have a lot of adverse weather in our area. We had a flash flood in April 2023 and we used our emergency communications system to warn the public."

Emergency management & business continuity, government administration, Canada

"Sitting in Europe, adverse weather looks very different from, say, North America or Asia Pacific. There's very active weather systems for North America and Asia Pacific, particularly hurricanes or typhoons. In previous years there have been big impacts from these hurricanes for our organization."

Crisis management, financial services, USA

"We've definitely triggered our emergency communication plan as a result of adverse weather. If we get a notification which is going to impact the health service, for example flooding, we would instigate our communications plans in relation to that. We've done that on a number of occasions."

Emergency planning manager, health sector, UK

IT or telecoms incidents were the second most common trigger for emergency communications plans, cited by 40.7% of respondents. As per Cloudflare's Year in Review[17], there were more than 180 global Internet outages in 2023, an increase of almost 20% year-on-year. An emerging trend is that many of these outages resulted from government-directed regional and national shutdowns of Internet connectivity. While some were brief, others were present for many months. Notably, government-mandated shutdowns in Manipur (India) and Amhara (Ethiopia) have been active for seven and four months respectively (at the time of writing). Furthermore, over the last 12 months there was also an increased number of service outages affecting major cloud providers such as Amazon Web Services, Microsoft, and Google.[18] An interviewee highlighted the risk of vendor outage to emergency communications which, in itself, should be a lesson to professionals to ensure the resilience of critical providers is assured and back-up is available if a provider has an issue.

> **"We had a technical implementation over a long weekend where certain key infrastructure individuals did not show up. We then had to very quickly reverse out that technical implementation. Sadly, that is the most common type of IT or telecom incident. The other time that happens is with software-as-a-service vendors. When there's some problem with the vendor, it interrupts our ability to use a key piece of our technical infrastructure."**
>
> Crisis management, insurance services, USA

Ranked third in the current year's table, 35.6% of activations were due to cyber security incidents and data breaches (2023: 34.4%). Although the number of attacks is still increasing globally (74.1% of practitioners in the BCI Cyber Resilience Report 2023 noted an increase in attacks over the past year), it is the increased sophistication, intelligent targeting of attacks, and social engineering methods which is resulting in organizations being impacted more deeply than previously.

Given this trend is likely to continue, particularly as criminals start to use AI as an additional attack vector, cyber security is set to remain one of the top triggers for activations in the near future.

> **"There have been a few cyber security incidents where we've had to instigate our emergency plans in relation to the loss of data."**
>
> Emergency planning manager, health sector, UK

> **"We had a ransomware attack against one of our key vendors, removing that vendor's ability to provide services to us. This would be something where we would need to get the critical infrastructure teams involved nearly immediately. We would have no control over what's happening at that vendor. We may have contractual agreements but in reality, cyber-attacks and ransomware attacks are not something that you can just flip a switch and recover from; it takes time."**
>
> Crisis management, insurance services, USA

Global conflict is also giving rise to sophisticated state-sponsored attacks. One of the most recent examples which had profound repercussions is the example of the Kyivstar attack on Ukraine in December 2023. Here, the country fell victim to a cyber-attack targeting its largest telecom operator, Kyivstar, resulting in extensive disruptions. Millions of individuals found themselves unable to access the Internet or make calls and, as a result, many chose to acquire new SIM cards from alternative providers. However, this sudden influx of new devices onto these networks led to service disruptions due to the heightened network usage. The impact rippled across various services, including banking and payment processing, affecting devices like ATMs that rely on SIM cards for connectivity. The fact that this attack affected so many communications systems, as well as banking platforms, shows the importance of having a system which is able to act independently of incumbent network systems.

IT incidents secure the fourth position, with more than one in four organizations having to activate their emergency communications plans due to such incidents (2023: 36.1%). Floods are in fifth place, with nearly one in five (19.5%) saying they had activated their plans as a result of flooding (2023: 22.8%). Critical infrastructure failure ranked in 6th place in 2024, with 18.6% needing to activate their emergency response plans for this.

> **"Our system was hacked. We couldn't access records, emails, anything. The entire server was gone and we didn't have a back-up. Now we have cloud computing, but then because of constant power failures, we sometimes lose information there as well."**
>
> Director, public services, South Africa

"We had a critical infrastructure failure a few years ago, when a local flood damaged one of the water supply pipes under the river and caused a water failure to the other side of the city as well as our hospital. It was a sunny day and a lot of rain fell in a short period of time around 90 kilometres upstream from the downtown. The speed with which the flooding occurred meant that our upstream gauges sounded the alarm too late and before we knew it the water was only a few inches under the lowest bridge. There was also a public event on one of the three bridges that day and we barely had time to close the roads before debris hit the side of the bridge."

Emergency management & business continuity, government administration, Canada

Interestingly, reasons for activation that were prominent a decade ago, namely natural disasters and fires, have seen a decline in their impact. In 2016, 44.5% and 42.1% of organizations had to initiate their emergency communications plans due to natural disasters and fires, respectively. However, in 2024, these figures have dropped, with only 8.5% of organizations activating their crisis plans due to natural disasters and 10.2% due to fires. Interviews spoke about the issues they had encountered when activating emergency communications plans.

"There's been numerous industrial action responses within the health services where we've had to instigate our emergency plans and crisis communication plans."

Emergency planning manager,
health sector, UK

"In Kyiv, Ukraine, we had a major mobile operator breach in December with two lots of eight days where services were unavailable and local transport collapsed. We then had massive missile attacks on December 29 and January 2; and 295 air raid alerts within 2023. We are still alive and 2023 was surprisingly successful for our business. Resilience works!"

CEO, professional services, Ukraine

"We had to activate our emergency communication plans for armed conflict, in relation to the conflict that's going on between Israel and Hamas at the moment. We do have a presence in that location so, when that started, we activated our corporate security plans. We're using regional response plans there as well."

Crisis management,
financial services, USA

Which of the following triggered your emergency or crisis communications plan in the past twelve months?

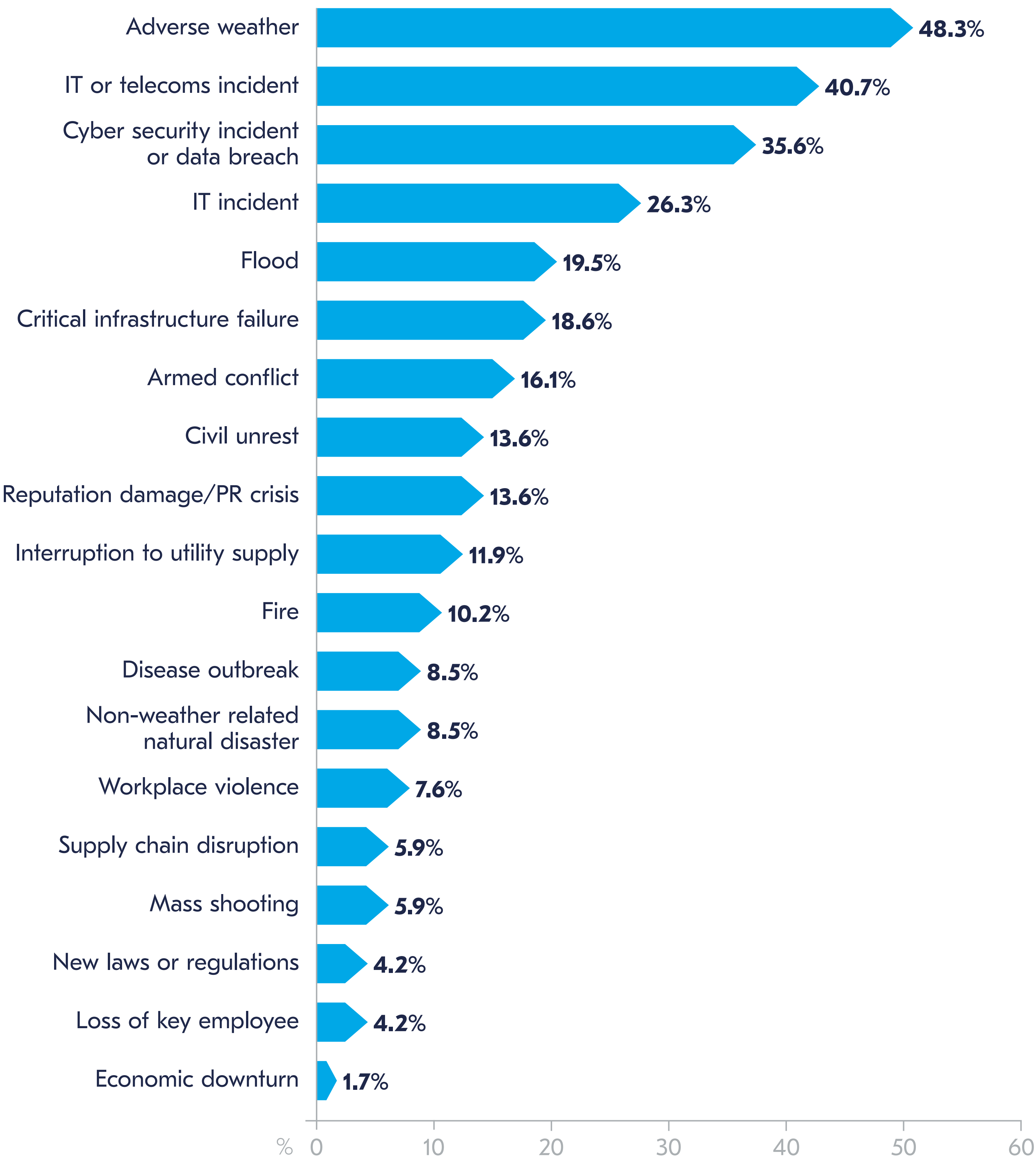


Figure 22. Which of the following triggered your emergency or crisis communications plan in the past twelve months?

Speed of response

Ensuring a plan can be activated quickly is crucial to its success. As has been the case for five years, most organizations (80.5%) are able to activate their plans within the 'golden hour' (60 minutes or less). However, the range of responses spanned from instantaneous activation, typically triggered by IT events or rules, to durations lasting a day. What is notable, however, is that the number of organizations able to respond within 30 minutes or less has fallen slightly this year to 67.7% (2023: 73.1%). Although this could be attributed to statistical variation, other reasons for this could be due to the increasing complexity of incidents, a more geographically diverse workforce, as well as an increase in the number of incidents occurring simultaneously. Furthermore, an increase in budget constraints means some organizations are returning to free solutions, or exploiting the capabilities of already-present enterprise software which could lead to a less effective response if not managed correctly. To emphasise this further, 27% of respondents could activate their plans within the 'golden five minutes' in 2023, whereas this year the percentage has fallen by over four percentage-points to 22.9%. Interviewees explained their reasons for their speed of emergency response, with human response capability being the prime disabler for quick communications.

> **"In case of a crisis, my response would be to get my mobile out, ring the executive direct, instigate the plan. That's why the response would be so fast."**
>
> Business continuity, charity sector, Australia

> **"When an incident occurs the information is automatically managed and then there is a triage phase where the information is sent to managers and the people involved that will verify the impact. It is for this reason that we take 5-30 minutes because when we are speaking about crisis, the part related to the emergency crisis can be automatically activated due to the fact that we have defined criteria. However, the next human stage takes a little bit of time."**
>
> Certification implementer, manufacturing sector, Italy

> **"If an event reaches a threshold, then we would immediately start a response. That would take between 5-30 minutes. This system still very much requires human involvement, which is why it can sometimes take a bit of time."**
>
> Crisis management, insurance services, USA

> **"We are getting a triage team together around whatever the emergency or crisis situation is. We have got a few different incident types and we've got automated alerts for those. Whether [the team] can join the call, of course, is another thing, but that's where we're using the automated system to pull people into a call. We just do the basic triaging step within that 5-30 minutes."**
>
> Crisis management, financial services, USA

> **"It would probably take a lot longer to activate our crisis plans if we were responding out-of-hours, because although we have our on-call teams, to then pull the right people together to confirm situational awareness and have the expertise, it's going to take considerably longer. I think we're good in-hours, not so good out-of-hours."**
>
> Emergency planning manager, health sector, UK

However, there are some positives to take this year, and one is the modest yet increasing number of organizations - now at a historical high of 2.9% - that can initiate their emergency plans instantly. This is a rise from 1.6% when this question was introduced into the survey in 2019 showing that new technology solutions are positively aiding incident response times.

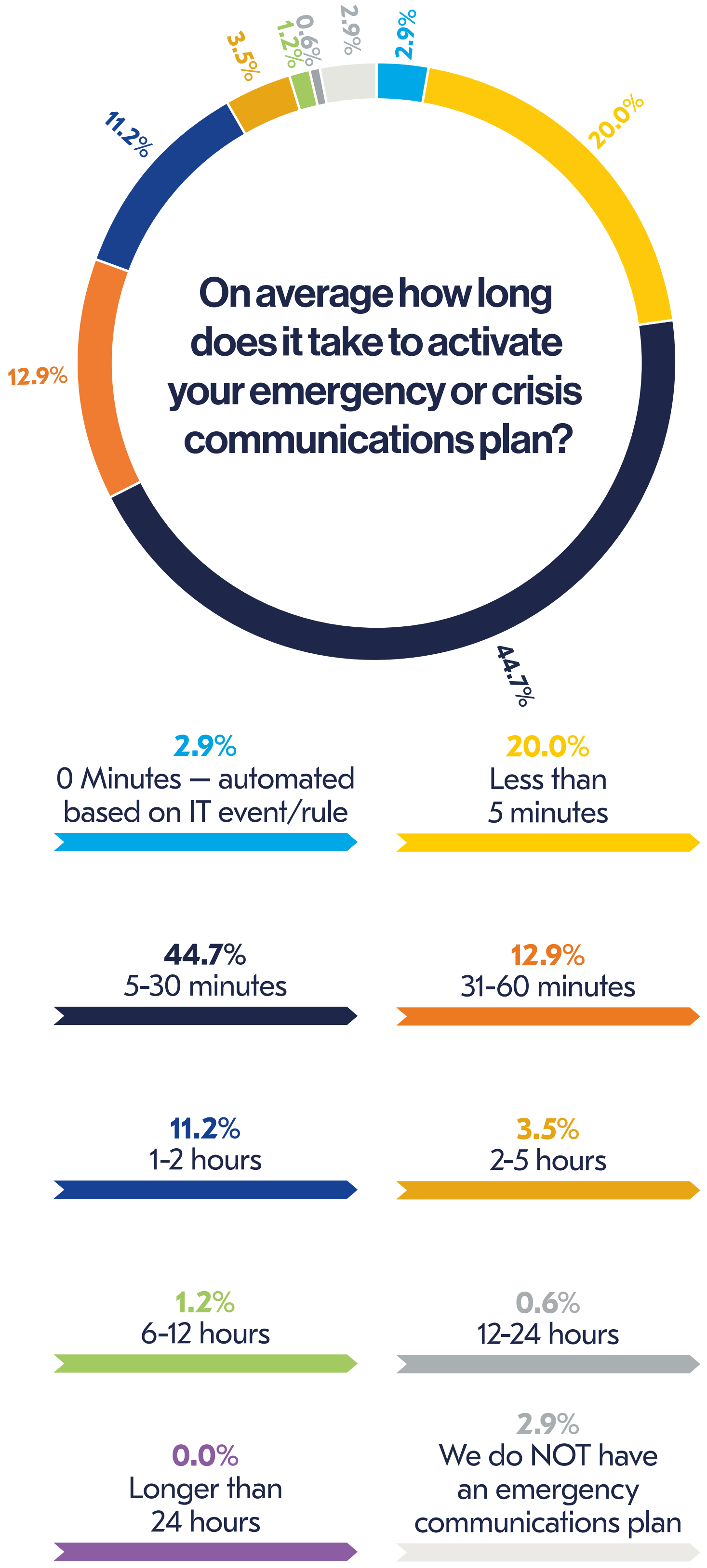


Figure 23. On average how long does it take to activate your emergency or crisis communications plan?

Activation time is proportional to the type of emergency communication solution employed by the organization. 84.8% of organizations who use dedicated emergency communications software can activate their plans within 60 minutes, 72.7% can do so in 30 minutes (2023: 77.2%), and a quarter (25.2%) are able to do so in five minutes (2023: 33.8%). Although speed has declined this year, the figures once again show that having a dedicated solution leads to faster activation. For those organizations without such tools or software, 69.2% can activate their plans within 60 minutes, just over half (57.6%) can do so within 30 minutes, and 17.0% can do so within five minutes.

Activation of emergency/crisis communication plans: with and without the use of emergency communication tools

	Organizations using an emergency communication tool	Organizations not using an emergency communication tool	% difference of those using a tool vs those who do not
Organizations able to activate plan within **5 minutes**	25.2%	17.0%	+8.2%
Organizations able to activate plan within **30 minutes**	72.7%	57.6%	+15.1%
Organizations able to activate plan within **60 minutes**	84.8%	69.2%	+15.6%

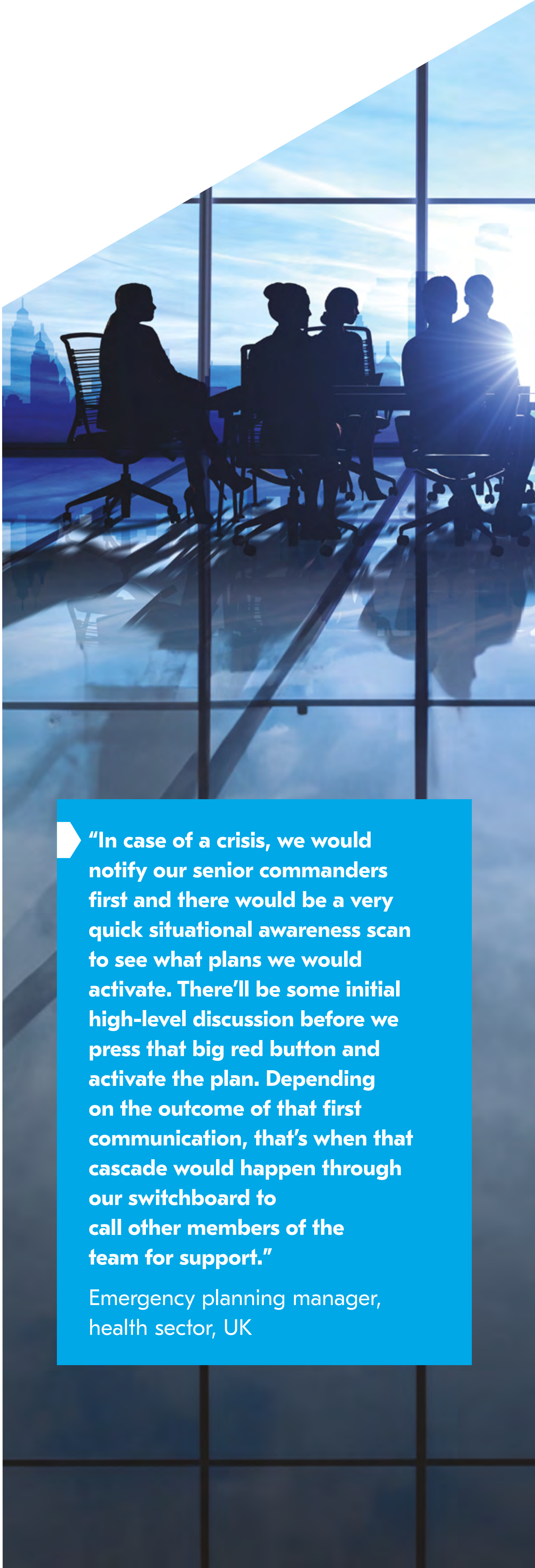
Figure 24. Activation of emergency/crisis communication plans: with and without the use of emergency communication tools

This table shows that SaaS or hybrid solutions are faster than on premises installed solutions: more organizations using either SaaS or hybrid solutions are able to activate their emergency communication plans within 5 minutes, compared to settings using on premises installed solutions. The same trend can be noted for the 30 minute period.

Activation of emergency/crisis communication plans: SaaS or hybrid vs on premises solution

	Organizations using an on premises solution	Organizations using a SaaS or hybrid solution	% difference of those using a tool vs those who do not
Organizations able to activate plan within **5 minutes**	18.7%	27.2%	+8.5%
Organizations able to activate plan within **30 minutes**	68.7%	75.3%	+6.6%

Figure 25. Activation of emergency/crisis communication plans: SaaS or hybrid vs on premises solution



The time it takes to provide information to top management is broadly similar to the time it takes to activate the plan. A significant majority (83.4%) can achieve this within an hour, almost three in five (57.4%) can accomplish it in under 30 minutes, while 11.8% are able to do so within five minutes.

The activation of emergency communication plans typically precedes the provision of information to senior management. However, it is worth noting that certain settings operate differently. According to several interviewees, they adopt a procedure where they first inform top management about a specific event and only once top management deems it to be a crisis can the relevant department activate the emergency communications plan. While this can prevent false alarms by ensuring accuracy and relevance, it is important to ensure that plans are in place should top management be unavailable to review information in a timely manner.

> **"The activation of the emergency communications plan occurs after we speak to our senior leaders who will decide whether we are activating or not, as well as which methods we'll use. We are always ready to get the notification out and have preset messages. That initial discussion before we decide takes between 5-30 minutes. However, once they say go, it takes us five minutes. It depends on the crisis though; if it's an active threat I would activate the emergency communications plan without asking first."**
>
> Emergency management & business continuity, government administration, Canada

> **"In case of a crisis, we would notify our senior commanders first and there would be a very quick situational awareness scan to see what plans we would activate. There'll be some initial high-level discussion before we press that big red button and activate the plan. Depending on the outcome of that first communication, that's when that cascade would happen through our switchboard to call other members of the team for support."**
>
> Emergency planning manager, health sector, UK

"If there is an event which is assessed and is bigger than originally appeared, that's when the senior management escalation occurs. Senior management expects us to begin the response before we reach out to them."

Crisis management,
insurance services, USA

"We will rarely bring in senior management before we have had the opportunity to bring together our incident response team, assign an incident commander, talk to subject matter experts, and assess the potential impact on the organization. This happens in the first 30 minutes after identifying that an event is taking place."

Crisis management,
insurance services, USA

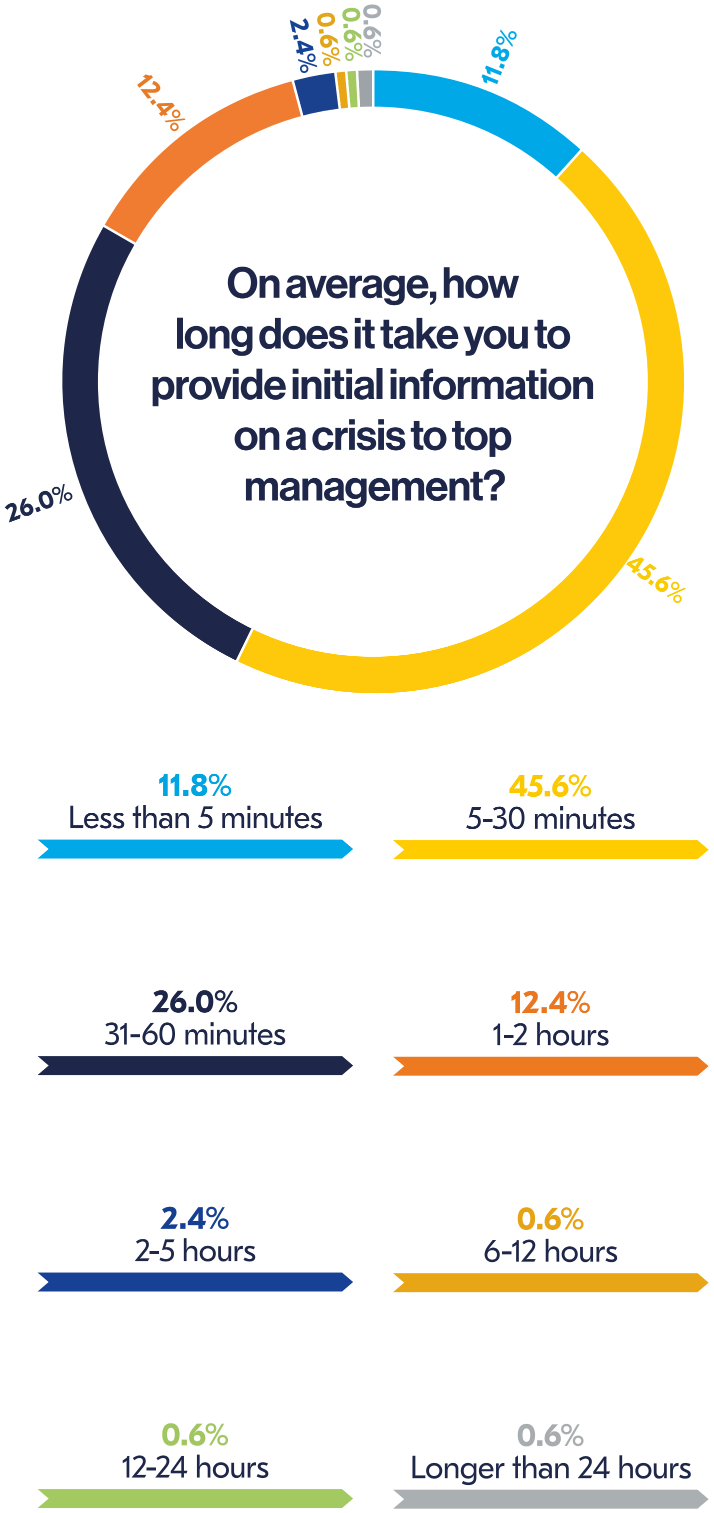


Figure 26. On average, how long does it take you to provide initial information on a crisis to top management?

Plans in action

Organizations achieved their expected response levels in 70.0% of activations, marking a decrease of 4.3 percentage points since the 2023 report. The decrease should not necessarily be perceived negatively, however. Many practitioners have introduced more sophisticated emergency communication systems in their work environments to effectively tackle the communication challenges faced today and, as a result, are introducing stricter targets for their tools to meet. This is further backed-up by survey comments confirming that organizations are imposing more ambitious targets which, as a result, are proving to be more demanding and challenging to achieve.

How often have you achieved your expected response levels?

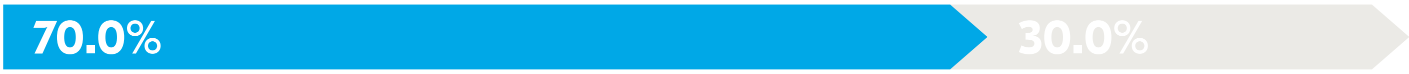


Figure 27. How often have you achieved your expected response levels?

As recognised in the speed of response section, the adoption of technology also influences the attainment of expected response levels. This year, 73.0% of organizations leveraging emergency communications technology met their anticipated response levels, contrasting with 65.0% of organizations not using a specific tool for emergency communications management.

However, while practitioners may be becoming more demanding of their systems, the 30.0% of organizations that failed to meet their expected response levels this year is notable. Carrying out regular training and exercising of emergency communications plans is instrumental in ensuring improved response levels. Interviewees explained the importance of reviewing an organization's culture in order to achieve better response levels.

> **"In terms of response levels, our systems aren't good. However, the response is actually reasonable because of the organization's culture. It's a very connected staff-based organization, and they are all used to talking to each other and stay connected. The response to an event happens naturally without a proper standardised system."**
>
> Business continuity, charity sector, Australia

> **"Our organization is quite large, and doesn't have a notification tool. However our response levels are quite high because normally we work close to each other so the news spreads via word of mouth."**
>
> Director, public services,
> South Africa

When you initiated your emergency communications plan, how often have you achieved your expected response levels? 2019-2024

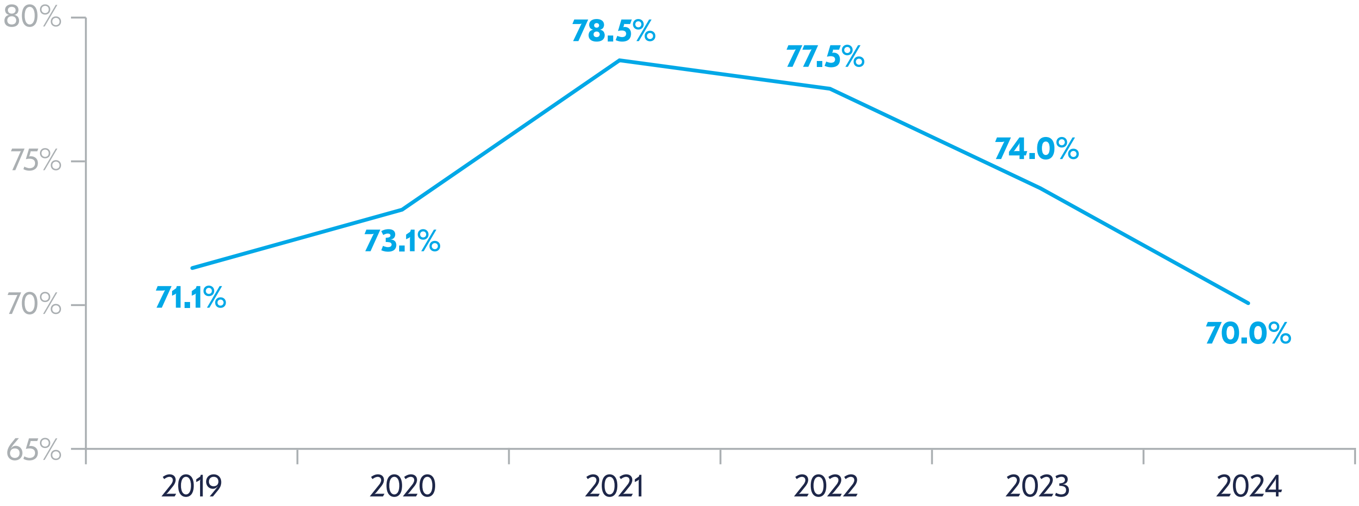


Figure 28. When you initiated your emergency communications plan, how often have you achieved your expected response levels? 2019-2024

The human element becomes a decisive factor when organizations fall short of reaching their anticipated response levels

Understanding the reasons behind response levels falling short of expectations is a crucial lesson for future improvements. BCI research consistently emphasises the concept that most shortcomings are attributed to human factors and procedural issues rather than inherent technological deficiencies. This year's data supports this.

According to respondents, the primary reason for the failure of crisis communication plans this year is a lack of response from recipients, selected by 63.4% of respondents, rising from second place in the 2023 report to first place in 2024. The success of an emergency or crisis communication plan is inherently dependent on the timely and effective response from recipients. One of the reasons for lack of response could be down to organizations reverting to tools that lack the functionality to provide read receipts, meaning that organizations fail to send out a secondary reminder via an alternative means. However, in order to improve response levels, organizations should not only ensure regular training and exercising of their staff, but also carry out regular test activations to ensure that messages are received and acted upon by staff.

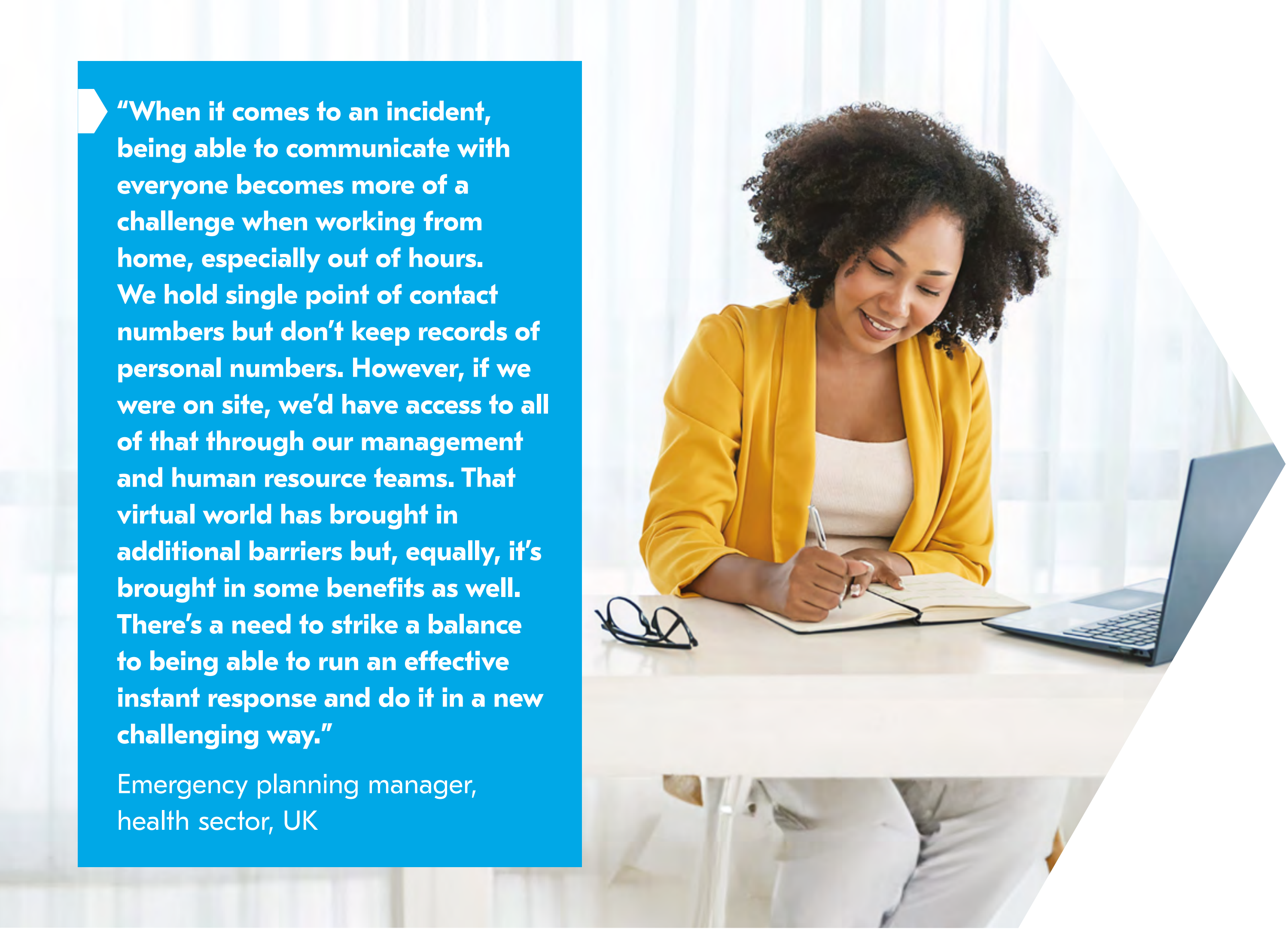
> **"Even though we only use our notification system for important or emergency communication, it is hard to get responses from recipients because people just think 'oh, it's another communication' and do not engage."**
>
> Emergency management & business continuity, government administration, Canada

> **"The lack of response from individuals who have been identified as subject matter experts is a key challenge for us. It happens fairly infrequently, but when it does it has had an outsized impact when we're still dealing with the incident. Until we have the right people in the room to help recover, we can't activate the right response."**
>
> Crisis management, insurance services, USA

> **"We have issues with getting people used to the drill of using the emergency texts as if it's a real message and not spam. I find quite an interesting difference between Europe and North America on this one. People in Europe are more sceptical, they think 'that's spam. I'm not going to answer that'. Whereas, in North America, they are, for whatever reason, more likely to respond, pick up, or acknowledge the message. It seems to be some sort of cultural difference between the two."**
>
> Crisis management, financial services, USA

Lack of staff contact information, selected by 41% of respondents, is the second most common reason for response times not being met. The Key Challenges section of this report addresses the challenges faced when attempting to interact with HR for contact information, often attributed to data privacy constraints.

Additionally, interviews for this report reveal the persistent practice of storing information in Excel spreadsheets is still commonplace, which hinders the implementation of the emergency response as information is not updated regularly or consistently, is siloed on different computers, and/or has issues with version control. Again, test activations can help to highlight which individuals do not receive emergency notifications, prompting them to update their details with HR.



"When it comes to an incident, being able to communicate with everyone becomes more of a challenge when working from home, especially out of hours. We hold single point of contact numbers but don't keep records of personal numbers. However, if we were on site, we'd have access to all of that through our management and human resource teams. That virtual world has brought in additional barriers but, equally, it's brought in some benefits as well. There's a need to strike a balance to being able to run an effective instant response and do it in a new challenging way."

Emergency planning manager,
health sector, UK

"Because we don't have documented emergency plans readily available, people might not know what to do in the event of an emergency."

Director, public services, South Africa

34.3% of respondents cited recipients' devices being switched off/unavailable as the reason emergency communications plans failed within their organizations. This issue is particularly prevalent where staff use personal devices for business communication and may ignore work related messages out of hours. Work devices can be better controlled by IT departments and allow for greater communication functionality during an incident. This scenario highlights the importance of understanding and respecting employees' privacy, while providing clear guidelines on device availability and implementing alternative communication strategies to ensure a swift and compliant crisis response.

Other issues relating to people were the failure of manual processes (23.1%), lack of technical expertise in using the process (22.4%), and problems communicating the urgency of the response (17.2%). Issues relating to technology, such as unavailability of the mobile network, internal IT failure, and device failure, are located at the bottom of the list.

"The reason why we're not achieving our expected response levels is probably because of the unavailability of the networks, because of our very rural location, and where our staff are located."

Emergency planning manager, health sector, UK

"There are still some places in the organization where there are a large number of manual processes and they're dependent on a very small number of individuals. So unfortunately we have key person risk in some areas that we find unacceptable. While these members of staff are usually more tenured, they're not as up-to-date on technology and, as they are dependent on technology that they don't fully understand for emergency situations, it means they depend much more on our IT teams. This, in turn, impacts our response levels."

Crisis management, insurance services, USA

If you failed to achieve your accepted response levels, what caused the failure?

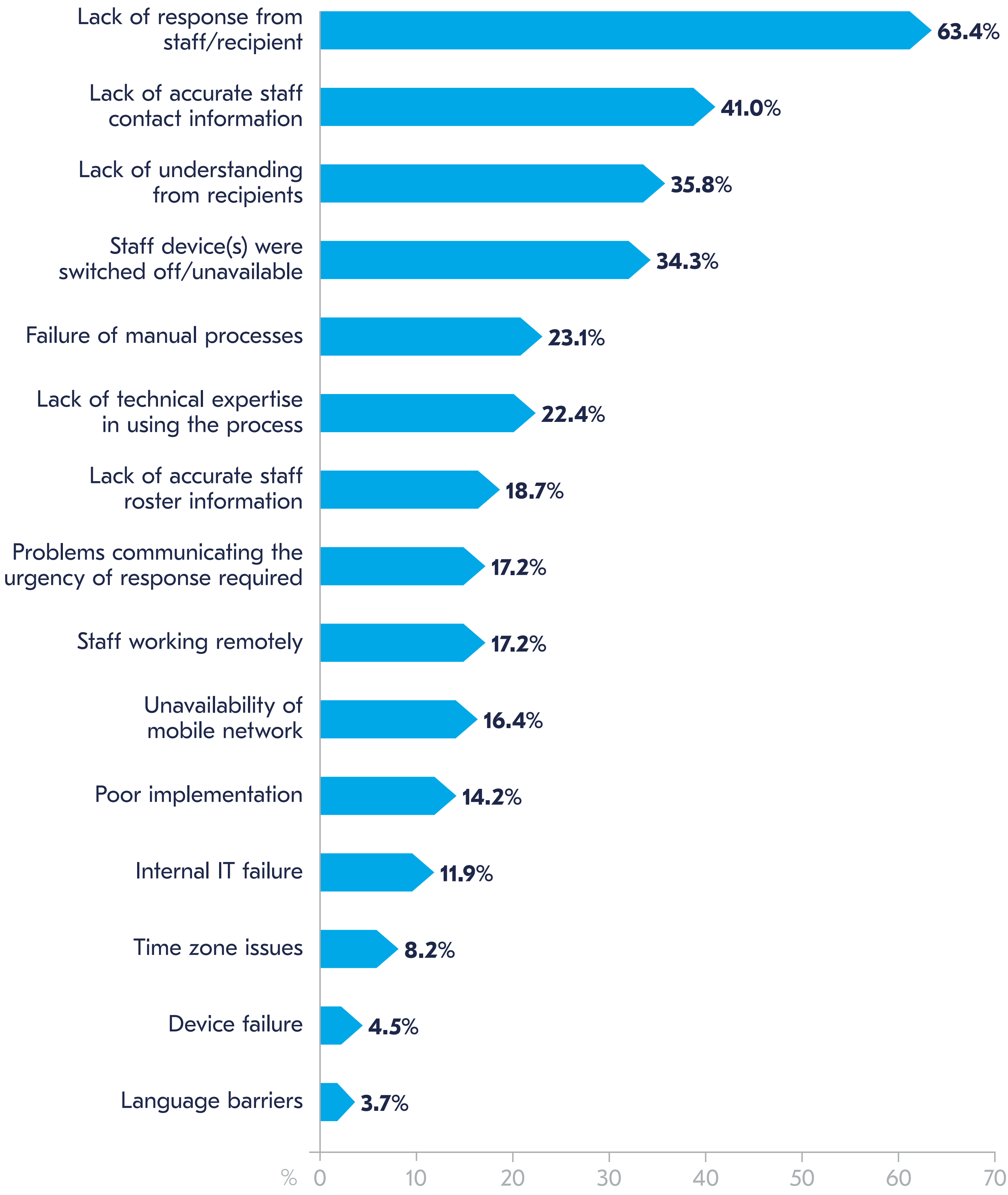


Figure 29. If you failed to achieve your accepted response levels, what caused the failure?

4

Key challenges

Key challenges

- Difficulties in obtaining accurate information quickly and efficiency during a crisis is the key challenge for practitioners. Locating staff is also an issue.
- Organizations do try to stay abreast of current developments through methods such as using weather forecasting apps and intelligently scanning social media, but also seek to collaborate with the wider community to share information and elicit a unified response.
- Keeping staff contact information up to date is also a key priority, showing awareness of the problem that incorrect staff contact information is a key reason for emergency communications plan failure.

Crises and emergencies are, by definition, challenging situations. The unique nature of crises means that, even with the best planning, organizations will face challenges when trying to initiate emergency communications plans. However, by being aware of the challenges faced, organizations can become better prepared to ensure that the common failures do not happen again.

The most common issue encountered is the ability to gather, validate, and share accurate information: with 35.1% of respondents selecting it as their top challenge. This issue has risen from fourth place in the table in the 2023 Emergency & Crisis Communications Report.

While this option is consistently near the top of the table, it is progressively becoming a bigger challenge. The sheer volume of information that can be collected during an incident can be difficult to navigate and this, coupled with fake news, disinformation campaigns, and social media reporting, adds additional complexity to the process of information gathering, validating, and sharing. As an example, four studies carried out by the World Health Organization (WHO) in 2022 showed that in social media posts during the pandemic, misinformation was found in 51% of posts about vaccines, 28.8% of posts about COVID-19, and in 60.0% of posts about pandemics[19]. As a result of such disinformation campaigns and the potential for information overload, senior management expectations in relation to incident management are becoming more demanding.

"In terms of gathering and validating information, at the moment the organization is storing information on a hard drive in a folder file system. Very clunky. Finding information and sharing that information is time-consuming and not ideal in a crisis scenario."

Business continuity, charity sector, Australia

"Under duress or emotional stress, stories go crazy and you're trying to determine what message to send out and who to send it to. External communications are not really centralised and people, teams, and managers deal with their own teams as they see fit."

Business continuity, charity sector, Australia

"Gathering, validating, and sharing accurate information is a challenge we have in Ukraine. Because we work during a war, our critical infrastructure is often attacked which means that communication tools are also under attack. For example, it can easily happen that one or two Internet providers aren't available because they have been attacked, requiring time to recover."

CEO, professional services, Ukraine

"We have a lot of quality issues regarding information within this conflict. You cannot trust by default any kind of communication: you need to check it and compare it with other sources. You need to gather different types of information coming from different channels and somehow organize this information and then make decisions. That is a challenge."

CEO, professional services, Ukraine

"Checking the validity of the information received is very important for our organization. The system that we have in place uses the media as a source. This means that in some cases we receive a huge amount of information, or event notifications, that is not exactly relevant for us. Also, sometimes the articles or the news that we receive are not accurate in terms of the detail."

Certification implementer, manufacturing sector, Italy

The challenge of disseminating precise information is also being exacerbated in some cases by difficulties in communicating with the appropriate individuals, emphasising the importance of having accurate staff contact information. This point leads to the second major challenge for professionals during a crisis: that of communicating with staff. This option was in first place last year, although the changes in percentages year-on-year are negligible. The challenges around staff communication are usually a result of messages being ignored, devices switched off or being unavailable, or contact information being out of date and users not receiving messages. Interviewees explained that some staff are unaware of how communications will reach them, so they often delete or dismiss emails/messages as they think they are phishing attacks. Such actions point to a lack of awareness and insufficient training/exercising rather than a technology-related issue and is a common theme noted throughout this report.

"Communicating with staff is always a challenge for us. I'm not sure how we can rectify it, but it's the issue of personal versus work devices and the way that people prefer to get communications. Some people still like to get paper communication, some want short messages and quick communications. Some do not want to use corporate devices after work, while others don't want anything from work on a personal device. So, it's just about keeping up to date with what people prefer and how they want to receive communication."

Emergency management & business continuity, government administration, Canada

Other problems relating to communicating with staff are bureaucratic communication schemes where there is a need to ask different areas of the organization for the deployment of an emergency communications tool, adding time and effort and sometimes impacting the effectiveness of the response. Interviewees referenced this issue.

"The notification software is actually owned by our top tier government, so they don't give us as much access to the system as we would like. So, for instance, if I want to change a template that goes out to the residents in my city, I have to go through them to do that, sometimes causing a delay. We have to pre-populate all of our incident plans to be ready. If anything falls outside of those pre-populated templates, there will be a delay in communication."

Emergency management & business continuity, government administration, Canada

"There are a lot of silos within the organization. Because we're a not-for-profit, funding comes from different sources and different programs have their own funding, their own reporting and owning of tools and processes. They get caught up in their own little world because of funding, impacting the response."

Business continuity, charity sector, Australia

Closely related to the second challenge within crisis management is the difficulty of locating staff, chosen by a smaller number of respondents, but still very relevant to those organizations who operate in challenging environments. While this is relatively straightforward for those on-site, for those in hybrid and remote working environments, communication becomes more complex, particularly during out-of-hours. Furthermore, the relatively slow uptake of satellite communications and other solutions (such as external antennae to boost in-building communications) that can negate the problems of communicating in network blackspots means that remote staff working in some areas can potentially be uncontactable. A two-way communication tool can expedite the issue, although consideration still needs to be made to communication procedures in the event of a network outage. Furthermore, some nations have strict privacy laws that inhibit organizations' capacity to store and make use of staff personal contact details to be able to locate staff during out-of-hours or when employees are on leave. Getting staff to follow planned procedures is also an important challenge for organizations, ranking in fourth place.

Less critical options for respondents during emergency notification/crisis management events include communicating with customers and other stakeholders; and communicating with staff members' next of kin. However, while other challenges may be towards the bottom of the table, for some interviewees, they can be critical in the effectiveness of the response.

"It is hard to get staff to follow planned procedures because a lot of procedures aren't formalised so the system isn't supporting it. The system is awkward, so standardising and the application of procedures just isn't there yet."

Business continuity, charity sector, Australia

"Getting staff to follow procedures is very difficult. It's like herding cats. We do a lot of training and we try to do a big in-person event at least twice a year. However, it's difficult because we also do remote work and many people don't come into the office anymore."

Emergency management & business continuity, government administration, Canada

"Documenting activities is something that is very hard to centralise as you need to gather information from different sources and centralise it in one platform. Additionally, you have changes in sources from project-to-project and, also, depending on the situation. That's why any kind of automatic tool has limited application for us."

CEO, professional services, Ukraine

“Effective communication with remote teams is actually really important for us because everybody’s remote these days. That’s either remote as in working from home, or in offices in disparate locations. Quite often, you’ll find that specialist teams are in, say, an Indian or a North American location and they’re the ones that you actually need to get together to respond to some event. This could also be across different tiers of the response. It’s a global company and it’s important that the response and the communication is consistent across each of the regions.”

Crisis management, financial services, USA

“We sometimes have people moving around different buildings and sometimes they are off-site. We don’t have data readily available for all the employees that are in one place, or who’s doing what somewhere else. For instance, if you walk into our main building, our access control system is broken. Instead we use a manual system and sometimes people don’t write their names down. You might find that in a case of emergency you think that you have a 1000 employees in the building when in fact you’ve got 1500.”

Director, public services,
South Africa

Top three key challenges during emergency notification/crisis management

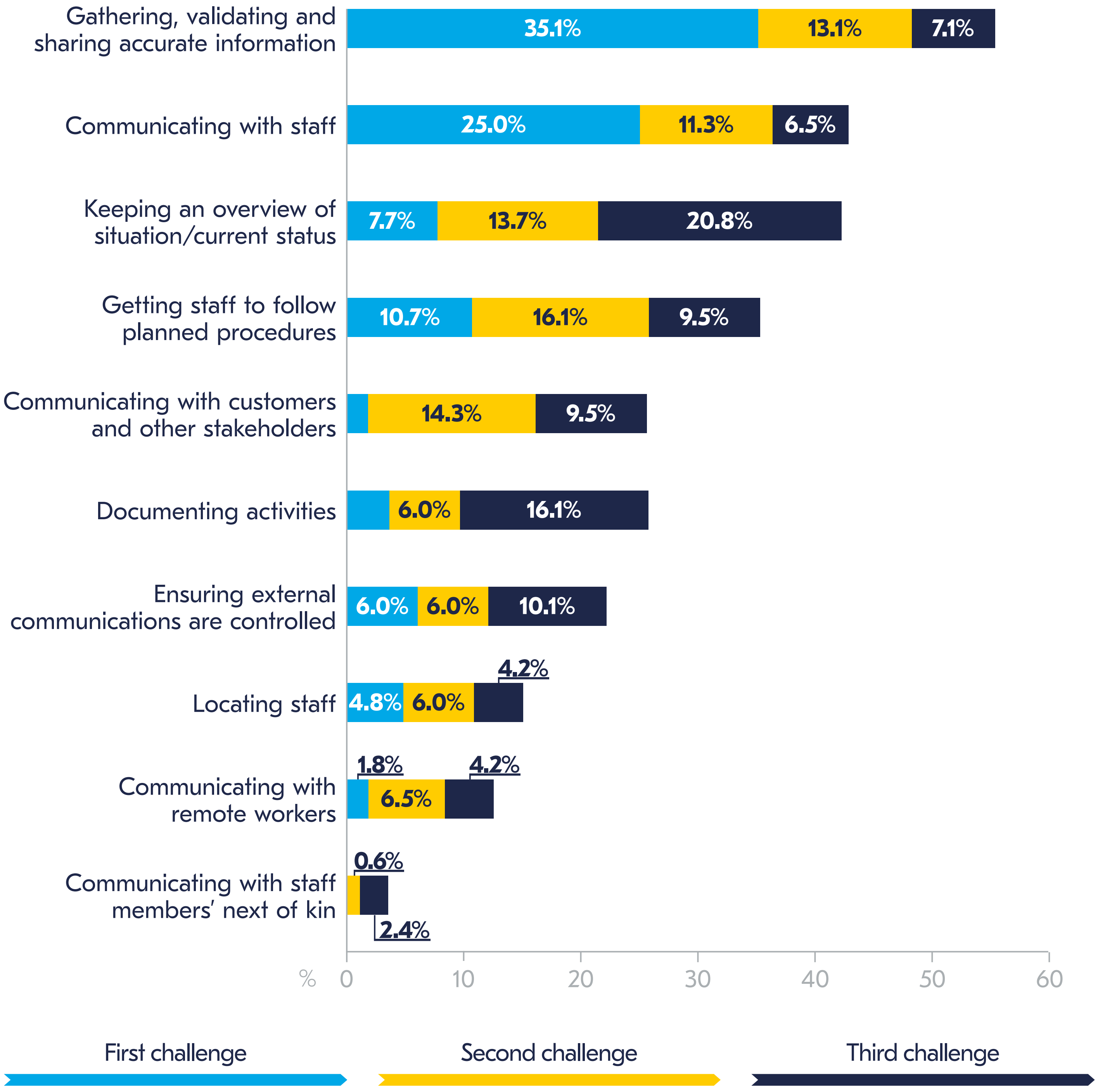


Figure 30. Top three key challenges during emergency notification/crisis management

Organizations use different ways of ensuring the acquisition of timely and accurate information

Gaining an understanding of the data sources used by organizations in a crisis can help to offer insights into why certain challenges become prominent.

Most organizations (64.7%) check weather alerts to ensure they are prepared for extreme weather events. While this is positive, most of the alerts are obtained using freely available data sources and the use of paid-for weather mapping applications is not as widespread. However, as weather events are becoming more frequent and more severe, there is also a growing trend of investing in corporate weather forecasting tools. Indeed, according to Acumen research and consulting, the global weather forecasting services market is growing at pace, driven by the rising demand for precise weather forecasts. In 2022, the size of the global weather forecasting services market was US$2.5 billion and it is projected to reach US$6.1 billion by 2032, demonstrating a compound annual growth rate of 9.4%.[20]

Second place in the table when it comes to ensuring the acquisition of timely and accurate information is the 62.5% of respondents who ensure that employees' contact details are up to date to guarantee that they can be reached in a crisis. However, with only two-thirds of respondents saying that they do this, it raises concerns and goes some way to explaining why incorrect staff contact information is so often a reason for plans failing. While some organizations may feel that system updates are automatic, with staff obliged to regularly fill in their contact details, regular checks and tests still need to be carried out to ensure that any errors are uncovered before causing a failure in a real-life crisis situation.

For some organizations, adopting a 'bottom up' approach in a crisis situation can help to inform the decision-making process and also prevent potential silos being built up between those on the ground responding to the crisis and senior management. It is therefore encouraging that more than half of respondents (56.6%) consider collaboration with local staff a critical element of their information gathering and response; and a similar number (54.4%) mention that communications between staff and management at the scene of a crisis is a vital part of their crisis response plan.

Checking official social media and media accounts is a method to ensure the acquisition of timely and accurate information favoured by more than half of respondents, while a third (33.1%) also use unofficial social media accounts too. While even official media sources often need to be verified, this is even more true for information gleaned from social media. However, mining social media for data during an acute crisis can help to provide up-to-the-minute information which can be extremely valuable in a mission-critical situation.

How do you ensure the acquisition of timely and reliable information when it comes to an incident or crisis situation?

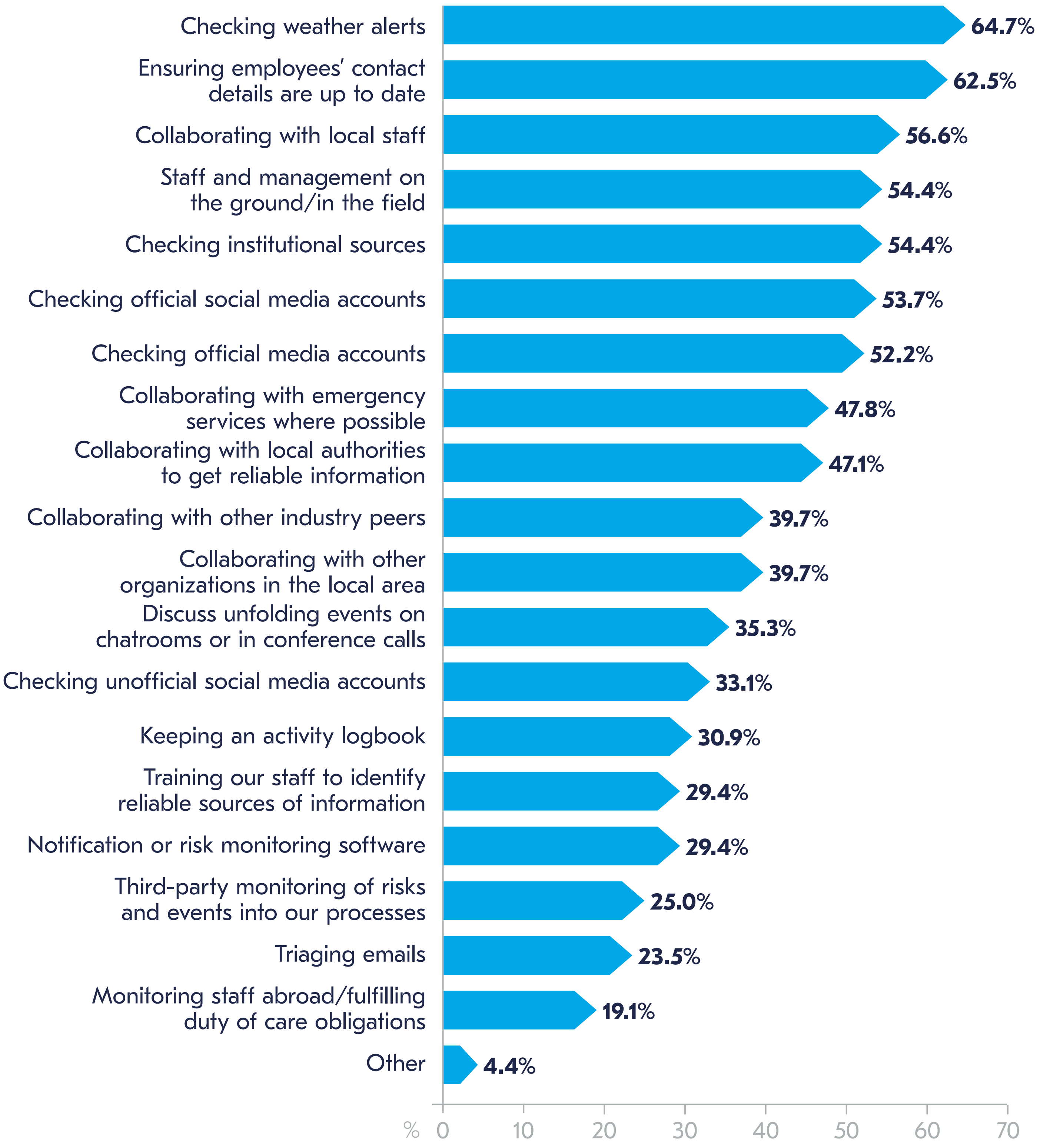


Figure 31. How do you ensure the acquisition of timely and reliable information when it comes to an incident or crisis situation?

Keeping employee contact details up to date

Keeping contact details up to date is clearly a problem for many organizations, particularly those that lack the funds to invest in a system to manage confidential staff information.

Historically, HR teams often operated in isolation, refraining from collaborating with other departments to ensure details were up to date. Contact information was typically stored in spreadsheets which led to data being siloed on individual machines, problems with version control, and giving rise to data privacy concerns. Siloed working practices are a common complaint of resilience professionals as these not only inhibit the ability to launch an effective emergency communications response, but also inhibit other aspects of an organization's resilience. For example, if the business impact analysis (BIA) process is carried out in compartmentalised silos, plans are not shared, work is duplicated, and departmental information lacks coherency.

"We need to find a way, even if it's monthly or regularly, to update contact information because people's contact details change. So we're using an old system where the contact information of employees are in their personnel files held by HR. So we need to find an electronic system that will enable us to get all the contact information and their next of kin, should there be a crisis."

Director, public services, South Africa

Progress is, however, being made: 46.3% of organizations now use automatic updates via an HR interface system as their primary method of keeping information up to date. Furthermore, there has also been a notable decline over the last five years in the use of manual lists to store staff information which, in itself, demonstrates that organizations are moving away from spreadsheets as a vehicle for data storage.

"We have a centralised HR system, which is a third-party application. The data in the system will be updated by the IT team. The communication application, which is a phone system, can only be accessed at work (on company mobile devices)."

Business continuity,
charity sector, Australia

"We use an interface with HR to keep data updated. After an exercise, HR will send out a general reminder to people to update their contact details. If we get someone who's repeatedly not done it, we'll follow up as well. But, obviously, with a big organization, there can be quite a few obstacles there."

Crisis management,
financial services, USA

Ensuring up to date contact data information: the use of manual lists is in decline 2019-2024

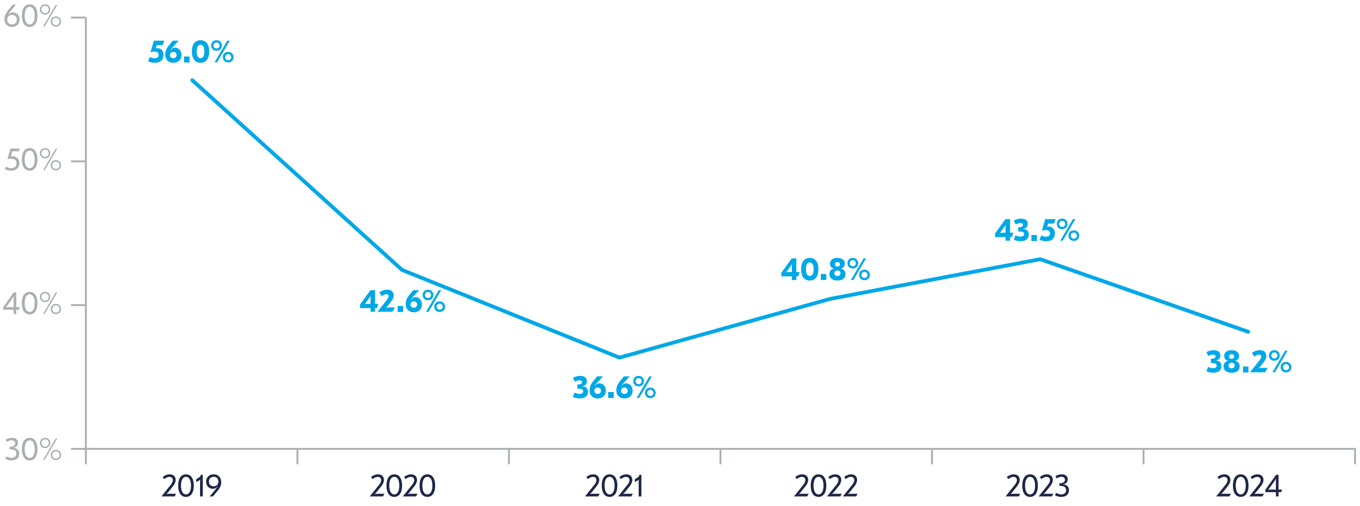


Figure 32. Ensuring up to date contact data information: percentage of respondents using manual lists

Another challenge already discussed in relation to data is some reluctance by staff to share contact details for out-of-hours scenarios. Although some countries do not have rules to protect employee confidentially, most do: and, as a result, many staff opt to exercise their right to keep this information confidential, even if it means unavailability during a crisis. Some organizations do, however, take a more stringent approach, mandating staff (typically at employment contract stage) to provide their contact details for use in emergency situations. Some organizations put the responsibility of updates to contact information on their staff which, if closely monitored and 'policed' effectively, can be effective.

> **"We use a massive communication tool within our organization. In some countries we have privacy restrictions and, due to the dimension of the organization, it is not so easy to maintain the data because we have so many different interfaces."**
>
> Certification implementer, manufacturing sector, Italy

> **"A challenge for us is how we hold our staff data and keep it updated and live to be able to let those emergency messages go out. Being able to communicate to staff outside GDPR governance is a huge stumbling block for us as an acute trust."**
>
> Emergency planning manager, health sector, UK

> **“From our organization’s point of view, it’s our responsibility as employees to update our personal data in our HR systems, which interface back out. We need really robust processes in place behind the scenes with our HR departments to make sure staff who are leaving are removed; and all that interfacing does need work. That’s where that collaboration with our IT becomes imperative.”**
>
> Emergency planning manager, health sector, UK

How do you ensure contact data of employees, experts, etc., is up to date?

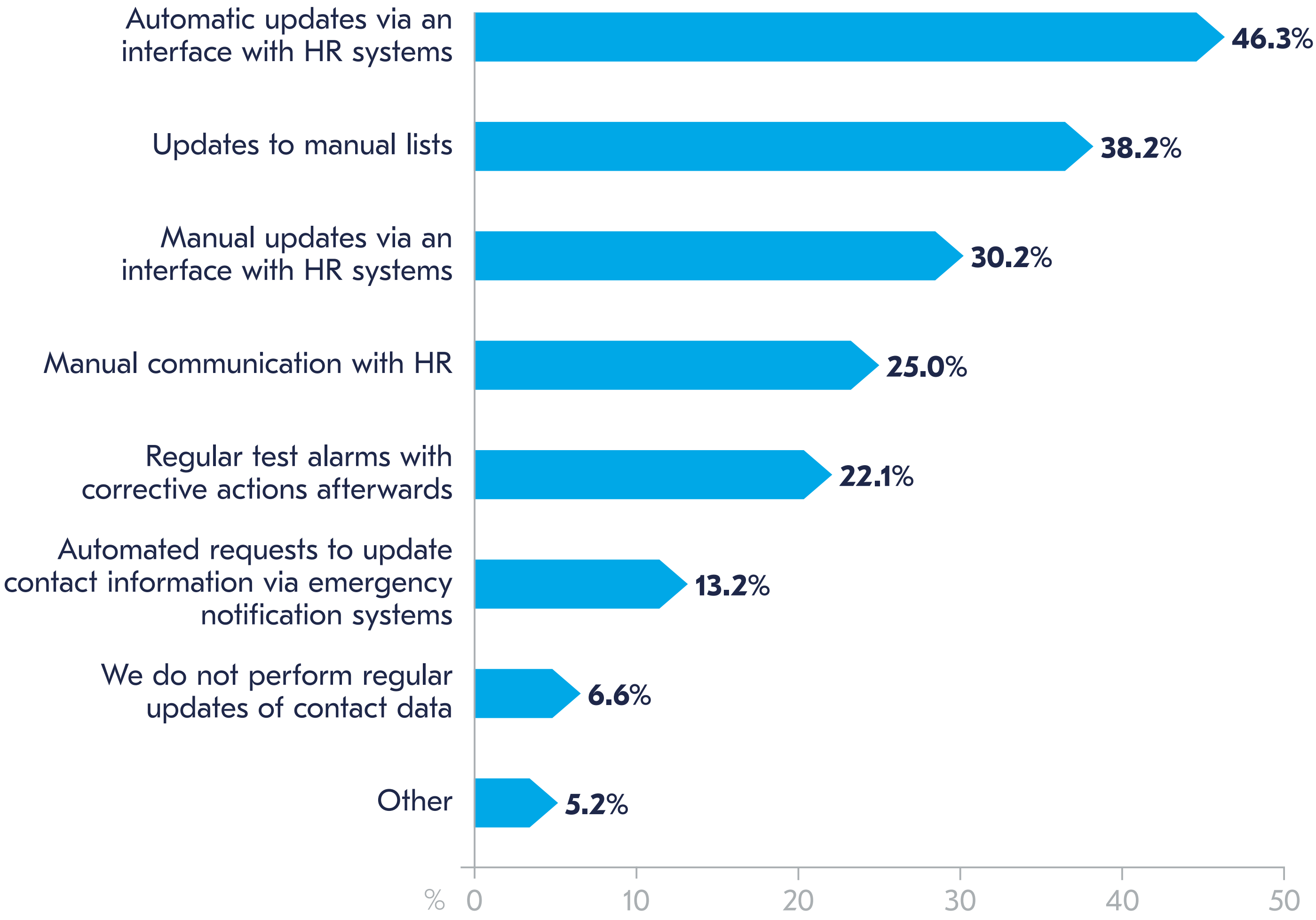


Figure 33. How do you ensure contact data of employees, experts, etc., is up to date?

5

Building resilience: training and exercising

Building resilience: training and exercising

- The percentage of organizations implementing regular training of their emergency communications is at an all-time high.
- Nearly half of organizations ensure that staff undertake training between two and twelve times a year (2023: 36.3%).
- Organizations are now exercising more, with most doing so at least twice a year.

This report has highlighted how training and exercising is key to ensuring successful initiation of emergency and crisis communications by helping to minimise failures relating to human error. Training and exercising does not just help staff to know what to do in the event of an activation, but it can also help to enforce the importance of every employee's role in a crisis. This in itself could help to solve one of the most fundamental issues in crisis communications discussed in the previous section – that of showcasing the importance of keeping personal contact information up to date.

While human errors are still very much at play when it comes to plan initiation failures, resilience professionals are becoming more aware of the need to carry out training activities. This is indicated in the 10-year data for this report (see Figure 34) which shows there has been a slow but steady increase in the amount of training taking place in organizations. In this sense, this year's data marks an all-time high in the running of regular training programmes. Hopefully, this will translate into better results for plan activations in next year's report.

Evolution of the development of regularly scheduled training programmes

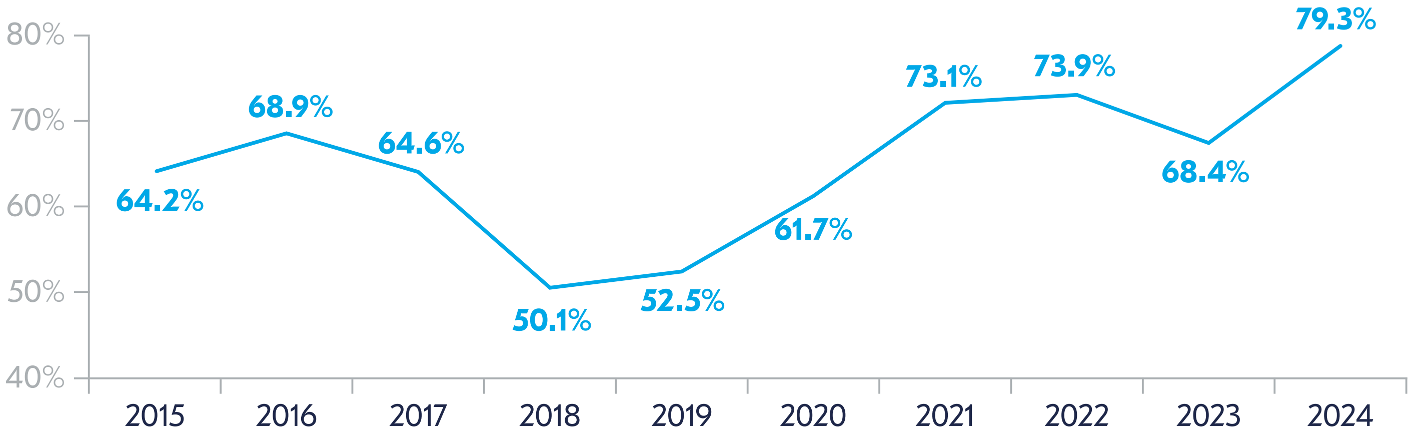
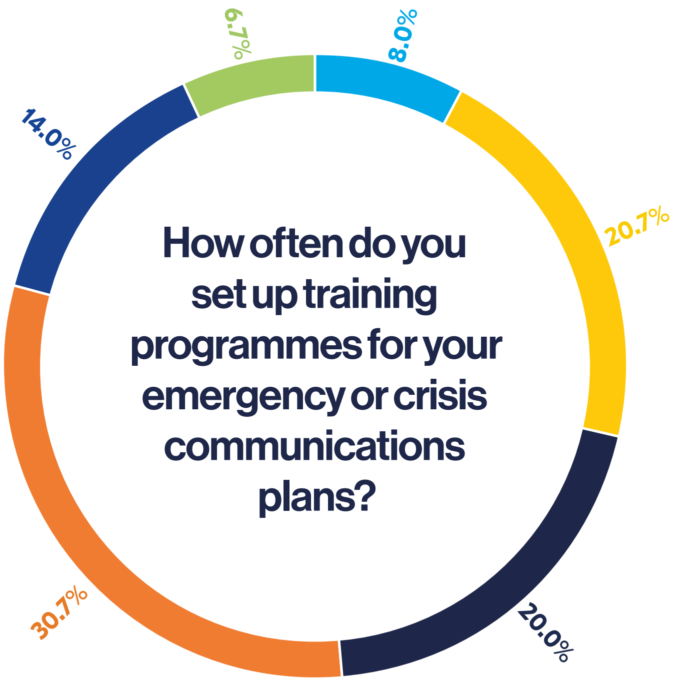


Figure 34. Evolution of the development of regularly scheduled training programmes within organizations 2015-2024

Furthermore, it is now widely recognised that carrying out training programmes once a year is far from sufficient and now, less than a third of organizations (30.7%) carry out annual training only. There has also been a notable increase in the frequency of training: almost half of organizations carry out training every six months or more frequently: 20.0% of organizations are training twice a year, another 20.7% are doing so every quarter, and a further 8.0% perform training monthly. Interviewees explained the kind of training they are performing within their own settings.



8.0%
Monthly or more frequently

20.7%
Quarterly

20.0%
Twice a year

30.7%
Once a year

14.0%
Less frequently than once a year

0.0%
Following an incident

6.7%
Never

Figure 35. How often do you set up training programmes for your emergency or crisis communications plans?

> **"We have two types of training within our organization. The first is computer-based learning that is pushed out to all of our employees across the world annually. This is mandatory training that reaffirms what their role is in business continuity. We also do a test to familiarise everybody in the firm with our emergency notification tool. We cover what it looks like to receive messages from that emergency notification tool and how urgently they must respond, so that everyone is familiar with it. We also require all of our business continuity teams to conduct training with their recovery teams that would recover the processes, technology, and staffing, for example."**
>
> Crisis management,
> insurance services, USA

> **"When we do emergency operations exercises, we do a large-scale exercise. Sometimes tabletops and sometimes 'live events'. We often partner with our neighbouring municipalities; with the police, fire, EMT, NGOs, utilities, and we get everybody to do the exercise together. This builds a comfort level between the different stakeholders and an understanding of the different roles of a large-scale response."**
>
> Emergency management & business continuity, government administration, Canada

> **"We did one virtual exercise in the past and it was very difficult for people to get their heads around doing a virtual exercise, so we now only do in-person exercising."**
>
> Emergency management & business continuity, government administration, Canada

Carrying out training after a real-life activation is now practised by more than half of organizations (56.7%). This ensures that learnings made from the post-incident review (PIR) or after-action review (AAR) can be added into training programmes so learnings can be made quickly, while still top-of-mind.

> **"After an event, gathering information on what went well and what did not can be a challenge because again, most of these records are kept manually and then have to be gathered centrally. This is because we do not currently have an incident management software that bridges all of those gaps."**
>
> Crisis management, insurance services, USA

> **"After an event, people don't sit down and look at what happened and what the lessons are that we can learn from this and other previous incidents, and make a plan going forward."**
>
> Director, public services, South Africa

> **"After an incident, we spend time deconstructing what went well and what did not go well. We focus on improving what we did well and we spend time with the involved incident management teams to do lessons learned and build a formal after-action plan that will close any gaps. If there are gaps identified that may cost money to fix and we don't have funding for them, then we take the matter to senior management as a risk. They must make the decision to either accept that risk or fund remediation."**
>
> Crisis management,
> insurance services, USA

However, some interviewees find challenges when trying to learn from past incidents.

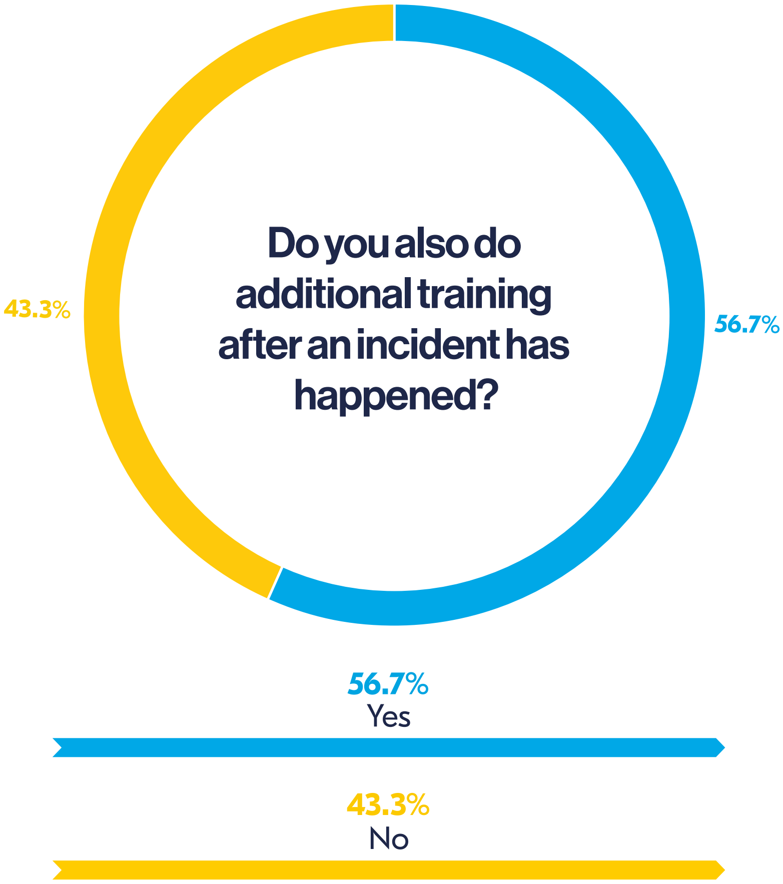


Figure 36. Do you also do additional training after an incident has happened?

Organizations are also exercising more and putting the training into practice

While training can help to ensure that staff know the processes and procedures to follow during an incident, exercising puts these learnings into practice and gives employees the muscle memory they need to be able to act appropriately in the event of a crisis.

Traditionally, organizations tended to run exercises once a year as taking staff away from their day jobs to take part in an exercise was looked upon unfavourably by senior management. Indeed, when reviewing the information from the first edition of the BCI Emergency & Crisis Communications Report in 2014, 55.8% exercised once a year, and just 12.0% did so two-five times a year. Figure 37 shows just how much training frequencies have grown, with this year's data showing that 39.5% of organizations carry out training 'more than once a year' and a lesser amount now carry out 'training once a year' (36.1%).

> **"We would run at least quarterly exercises to test the cascade of information when in a crisis. We would then build on that cascade to do the next stage of the incident response. We would do a focused exercise, usually a tabletop exercise based on a scenario."**
>
> Emergency planning manager, health sector, UK

Frequency of exercising of emergency communications plans 2015-2024

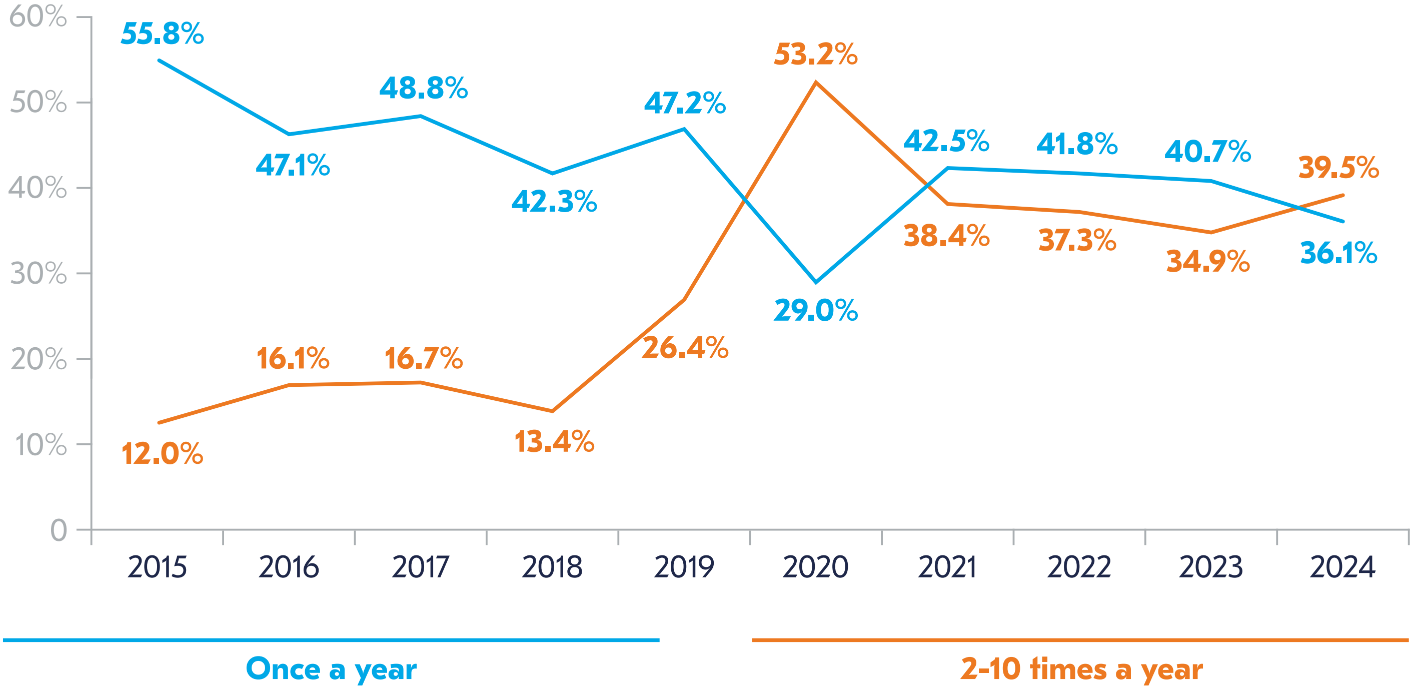


Figure 37. Frequency of exercising of emergency communications plans 2015-2024

It should be noted that, while most organizations are exercising more often, a concerning statistic has emerged in this year's data: the number of organizations training less than once a year has surged to 15.7% (2023: 7.2%), doubling in 12 months. Interviewees commented that a reason for this was moving to virtual environments negating the need for on-site testing. However, crises can still happen when staff are remote (e.g. cyber-attacks, death of a senior employee, network outages) and exercising should still be taking place. Some organizations are taking the opportunity to introduce virtual exercising into their workplaces which can provide opportunities for remote staff to participate and negating the need to travel to a physical location.

As organizations look to fully exploit newer methods of training to suit their own needs (such as online training), it is likely that some organizations will start to shift away from more traditional training techniques. However, this is not likely to happen just yet, as traditional training and exercising methods are still the primary mediums used in organizations: tabletop exercising is at the top of the list (73.3%), followed by alerting tests (63.0%), and focused exercising involving selected departments (61.6%).

However, as mentioned above, organizations are starting to leverage new technologies within their exercising activities: 30.8% of settings are performing simulation exercising, for example. This can help to train staff in scenarios typical to their organization and ensure that employees know what to do in specific circumstances. Furthermore, with artificial intelligence (AI) now being used within some simulation products, scenarios can become even more realistic to ensure staff are even better trained at reacting to the unexpected.

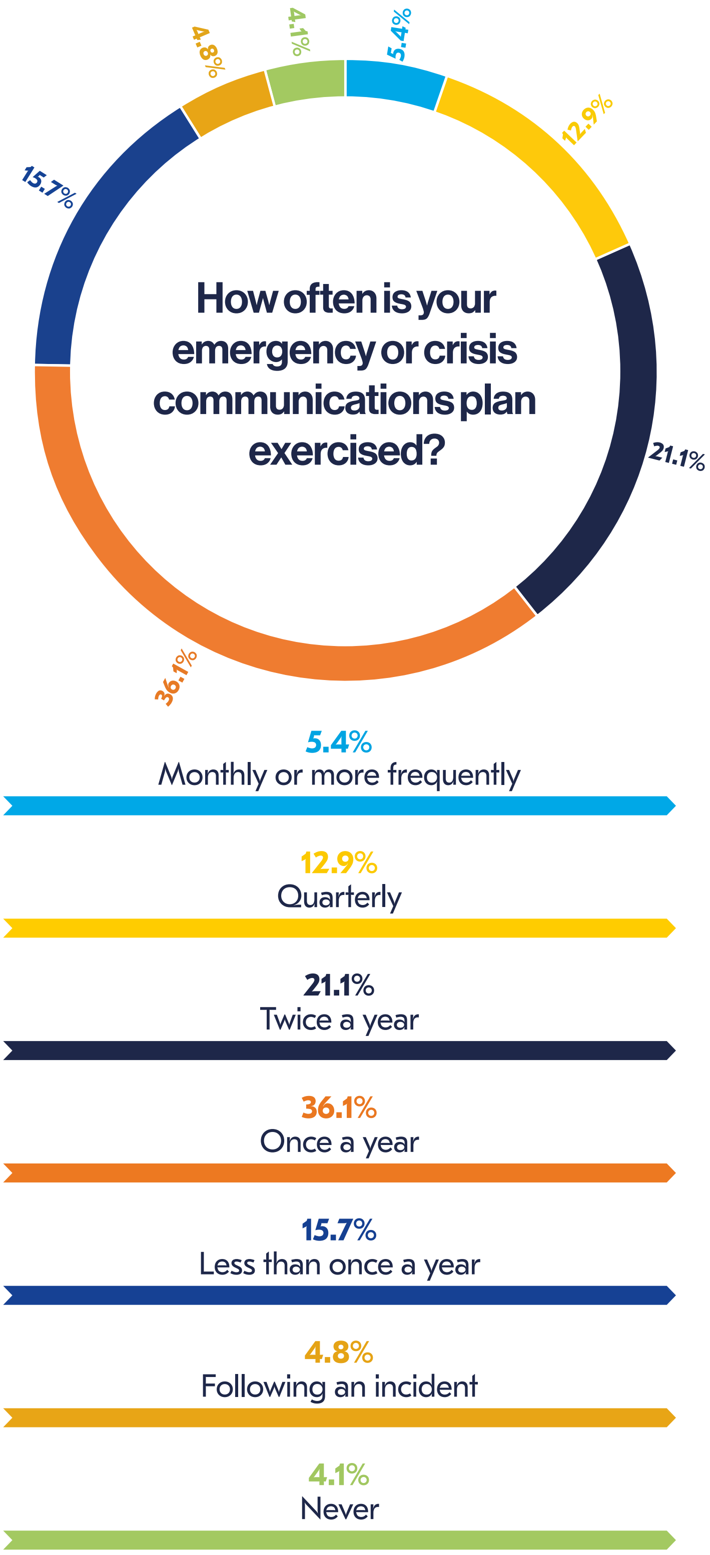


Figure 38. How often is your emergency or crisis communications plan exercised?

Which kind of exercising do you perform within your setting?

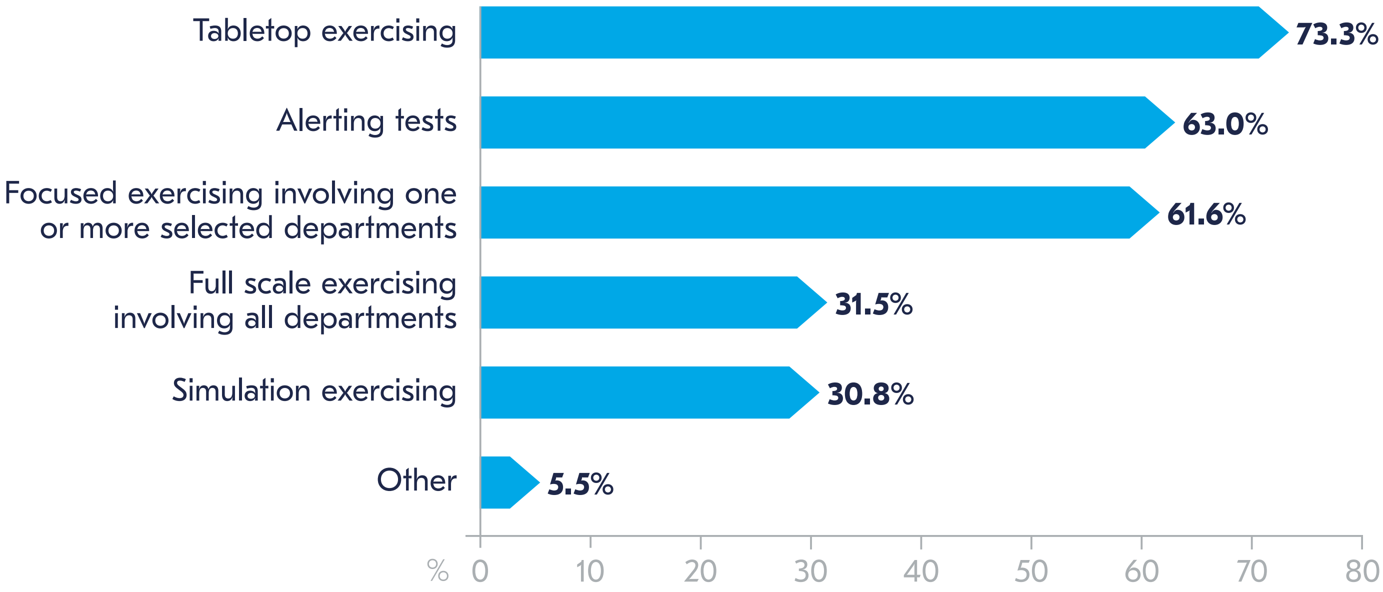


Figure 39. Which kind of exercising do you perform within your setting?

6

Internet of Things (IoT)

Internet of Things (IoT)

- The use of Internet-of-Things (IoT) devices is still low, but usage is now at a historical high.
- Although IoT devices can be greatly beneficial in emergency situations (e.g. early warnings), usage remains limited.

Incorporating IoT devices can be invaluable in some settings. In earthquake-prone communities, for example, sensors can detect earthquakes minutes or seconds before they happen, linking to alarm and public address systems and providing people with valuable time to get to a safe area. Japan, which suffered a serious earthquake on 1 January 2024, is one of the sixteen nations globally that has an early warning system in place to allow people time to make themselves safe. Another nation which has an advanced system in place is Mexico, where videos are freely available showing the effectiveness of the system in evacuation procedures[21]. Similar systems can also be used for other incidents such as floods, chemical leaks, or fires.

Respondents' data suggests that the adoption of IoT in communication and crisis response is still an emerging concept — at least in private organizations — with most respondents being unsure of how such devices could benefit their own organizations. However, there is a slight uptick in usage when comparing this year's figures. Excluding those who are 'unsure', over a quarter (26.2%) of organizations are now using IoT devices to some extent within their emergency communications environment (2023: 24.9%). Furthermore, an additional 15.0% say they are planning to embed them in future (2023: 14.2%). Although these are only modest increases, it does show that practitioners are becoming more aware of the advantages of employing such devices and, as more devices become available at costs which are not prohibitive to organizations, IoT usage is likely to rise further.

An interviewee explained the use of IoT within their organization.

> **"The use of IoT within the organization comes down to server room monitoring and sensors that we've got in there to make sure individual server rooms are at the right temperature. There's also things linked to UPS and power that will tell us when they go down. These help us to initiate that immediate notification for someone to investigate and, potentially, turns them into a first responder."**
>
> Crisis management, financial services, USA

Use of IoT within emergency communications plans; 2019-2024

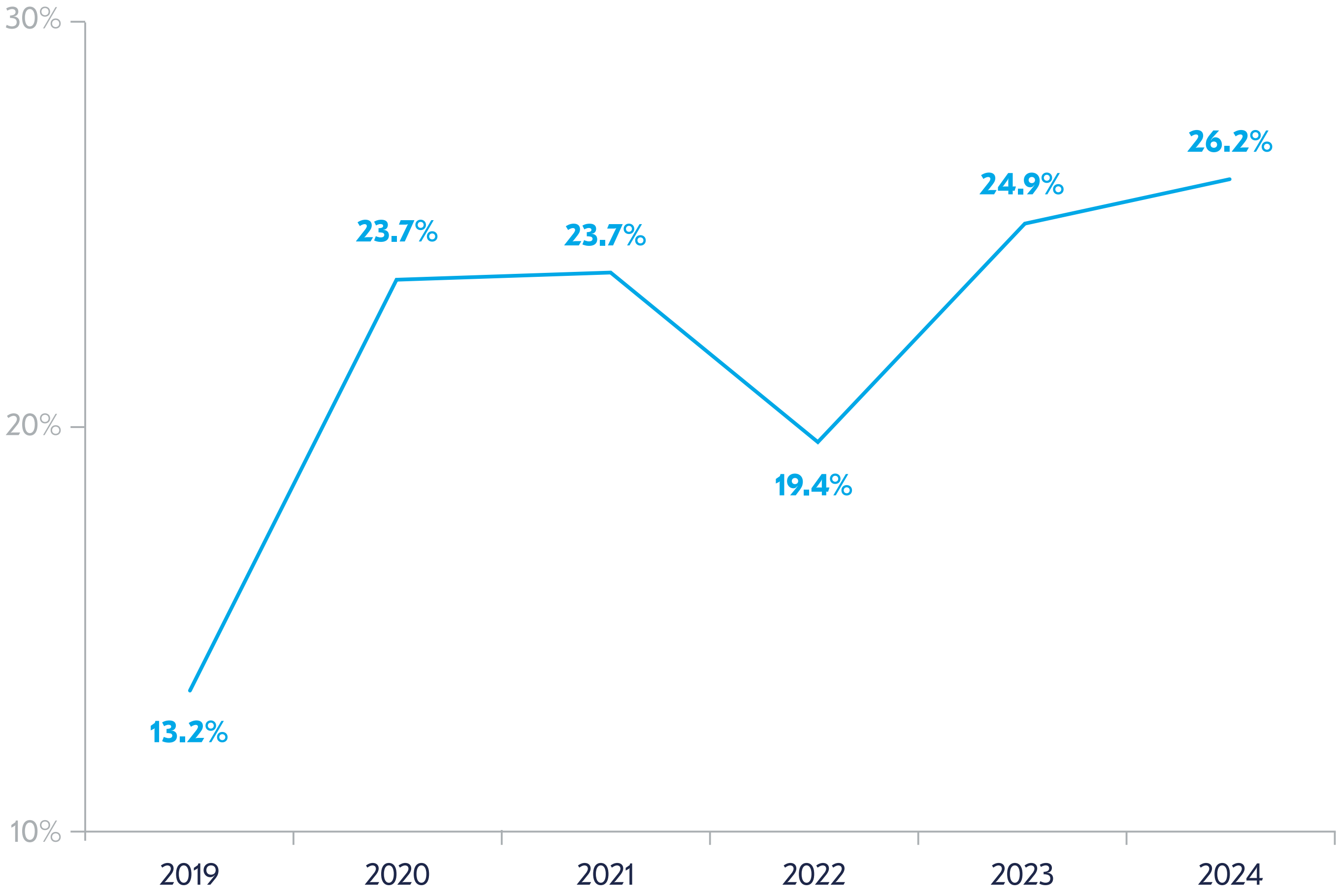
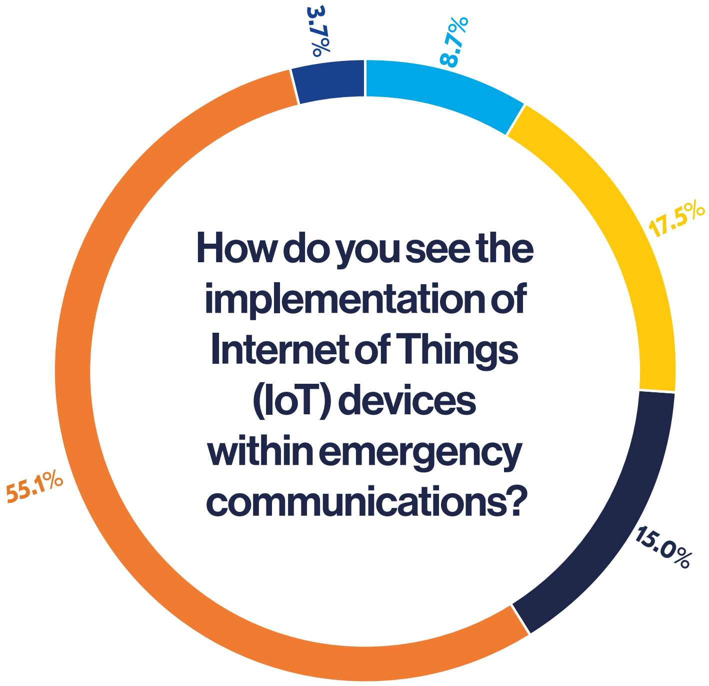


Figure 40. Use of IoT within emergency communications plans; 2019-2024 (percentage of respondents answering 'they are well embedded' or they are embedded in 'limited areas')



8.7%
IoT devices are well embedded in our emergency communications plan

17.5%
We use IoT devices in limited areas of our plan

15.0%
We are planning to embed IoT devices into our emergency communications plan

55.1%
We are not planning to embed IoT devices into our emergency communications plan

3.7%
Other

Figure 41. How do you see the implementation of Internet of Things (IoT) devices within emergency communications?

It is somewhat counterintuitive that, while most respondents consider IoT to be something that is either easy or manageable to implement into an organization's emergency communications set-up, most are either not planning to embed these devices into their emergency plan or are unsure whether they will. An interviewee suggested that cultural issues could be the reason their organization is holding back.

> **"Our main challenge in the introduction of Internet-of-Things is the silos we function in. When it comes to this type of emergency, people tend to be hesitant to share when they have an emergency alert. They think they're going to be judged because of it. For us, having an IoT system where you vocalise that there's something happening in your area is still a challenge, even internally."**
>
> Emergency management & business continuity, government administration, Canada

Data suggests that most practitioners are unaware of the benefits that IoT can bring to a programme or are perhaps using the technology without realising it (e.g. security monitoring systems). Some of the comments received from survey respondents shed some light on this.

"I don't really understand IoT," was one respondent's comments, and others commented that "[they were] not aware of how the integration methodology can be done", or had "not spent any time evaluating [it]".

Other respondents put out various reasons for not employing the technologies within their workplaces, with some believing it was too high a risk or there were security concerns to consider.

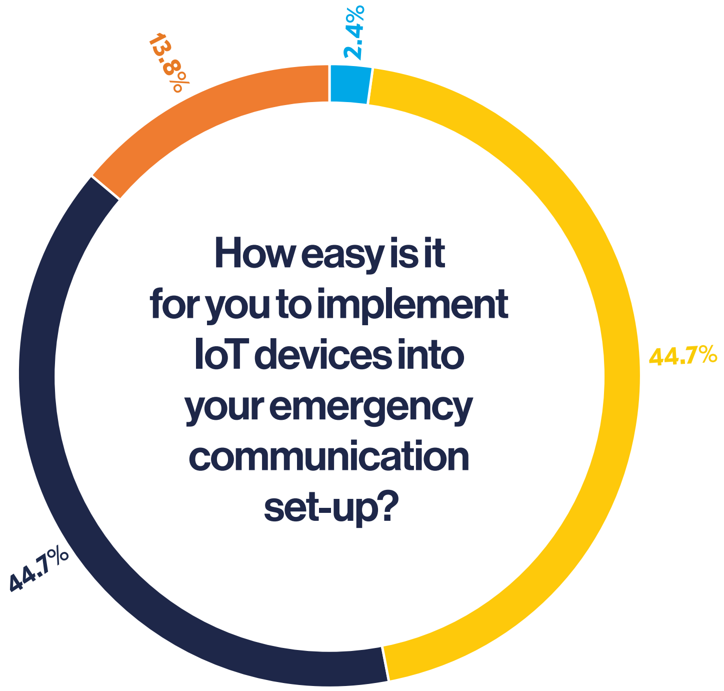
"Risk assessment considers it undesirable."

"As we already have modern fire alarms, fire protection, and security systems we don't see the point in reducing our device security by unnecessarily connecting devices with other unrelated systems."

"We do not have an automated system to allow us to implement this."

"It is feasible, but, culturally and from a cost perspective, IoT integration is a non-starter for our firm."

> **"Different silos are needed for setup and maintaining IoT devices. Also, there are security concerns because of poor software and patch-processes needed for IoT devices."**



2.4%
Very easy

44.7%
Manageable

39.0%
Difficult

13.8%
Not possible

Figure 42. How easy is it for you to implement IoT devices into your emergency communication set-up?

The emergency and crisis communications field over the last decade -

Digitalisation of the emergency response: the use of mobile phones has become the main tool to disseminate emergency alerts. The increasing use of mobile technology and social media platforms has transformed the way emergency information is gathered and disseminated. Authorities and organizations leverage a wide range of platforms such as Telegram, X, Facebook, Instagram, and other channels to collect information and provide real-time updates during crises. Social media platforms also enable community engagement, allowing people to share information and report incidents in real-time.

Increased use of new technologies: the use of data analytics and predictive modelling has become more prevalent. Analysing large datasets helps emergency management professionals make informed decisions and allocate resources effectively. Some of the applications of new technologies within crisis management includes predicting the spread of diseases, assessing natural disaster risks, and planning responses accordingly. AI and machine learning technologies are also being employed to analyse vast amounts of data very quickly. This assists in early detection, response planning, and resource allocation during crises. AI tools can also help in automating certain aspects of emergency communications.

Increased usage of applications to broadcast emergency alerts: many organizations have developed and adopted mobile applications to deliver emergency alerts and notifications directly to individuals. These apps provide location-based information, safety tips, and real-time updates during emergencies.

Importance of two-way communication: there is a growing emphasis on two-way communication between organizations and different stakeholders. This bidirectional communication helps in making sure that recipients are getting different alerts and helps organizations gather feedback by obtaining real-time on-the-ground information.

Collaboration with the community during a crisis is a key element of the emergency response: there has been progression in collaboration between different entities during a crisis as a key element of the response. The sharing of information and efforts has become more crucial in responding to emergencies, such as pandemics and climate-related disasters. Organizations and public bodies are increasingly working together to share best practices, resources, and information.

Cyber security concerns: with the increasing reliance on digital communication, there is growing awareness of the need for robust cyber security measures to protect communication infrastructure during emergencies. Cyber threats pose risks to the integrity and availability of emergency communication systems.

Over dependency on digital tools may be compromising the resilience of organizations when dealing with a crisis: organizations are moving towards a complete digitalisation of operations, making their existence reliant on having access to the Internet. Very few organizations are able to keep functioning while experiencing an Internet or long-running power outage (since many organizations have UPSs, at least, to deal with short power outages).

Training and exercising programs have become more sophisticated: helping emergency responders and communication professionals practice in a much more efficient way and helping them refine their crisis communication strategies. This includes an increased use of simulation exercises for managing communication in various crisis scenarios. The new working environment has forced organizations to embrace technology within the training and exercising sphere.

Increased public awareness and education in relation to crisis: efforts to educate the public on emergency preparedness and communication have intensified. Organizations are investing in awareness campaigns to ensure that their workforce is well-informed and knows how to receive and respond to emergency communications.

Annex

23 Oct to 19 Nov 2023

Survey dates

222

Respondents

51

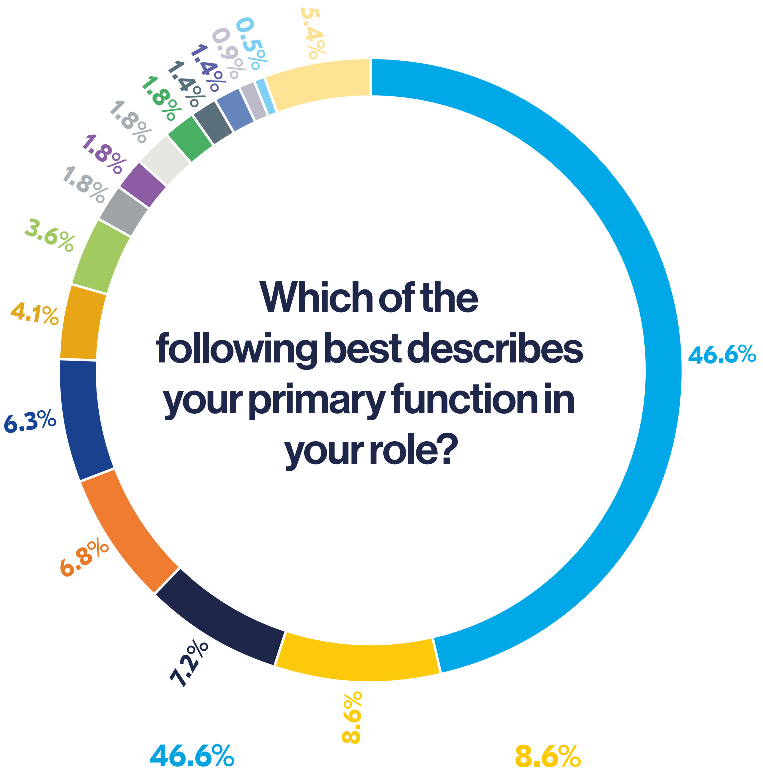
Countries

15

Sectors

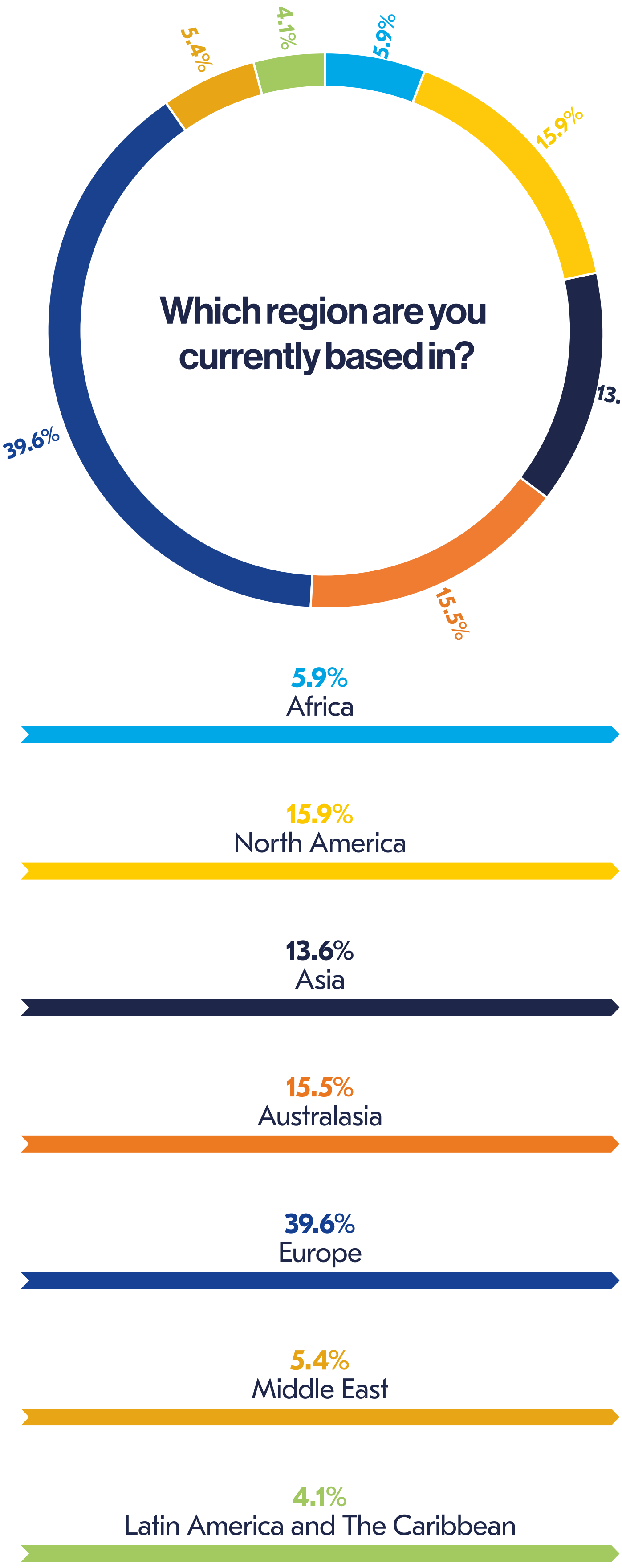
10

Respondent interviews



46.6% Business continuity	8.6% Risk management
7.2% Organizational resilience	6.8% Operational resilience
6.3% Crisis management	4.1% Top management
3.6% Emergency planning	1.8% Health and safety management
1.8% Operations/facilities	1.8% Information security
1.8% Internal audit	1.4% IT disaster recovery/ IT service continuity
1.4% Physical security	0.9% Communications
0.5% Quality/business improvement	5.4% Other

Figure 43. Which of the following best describes your primary function in your role?



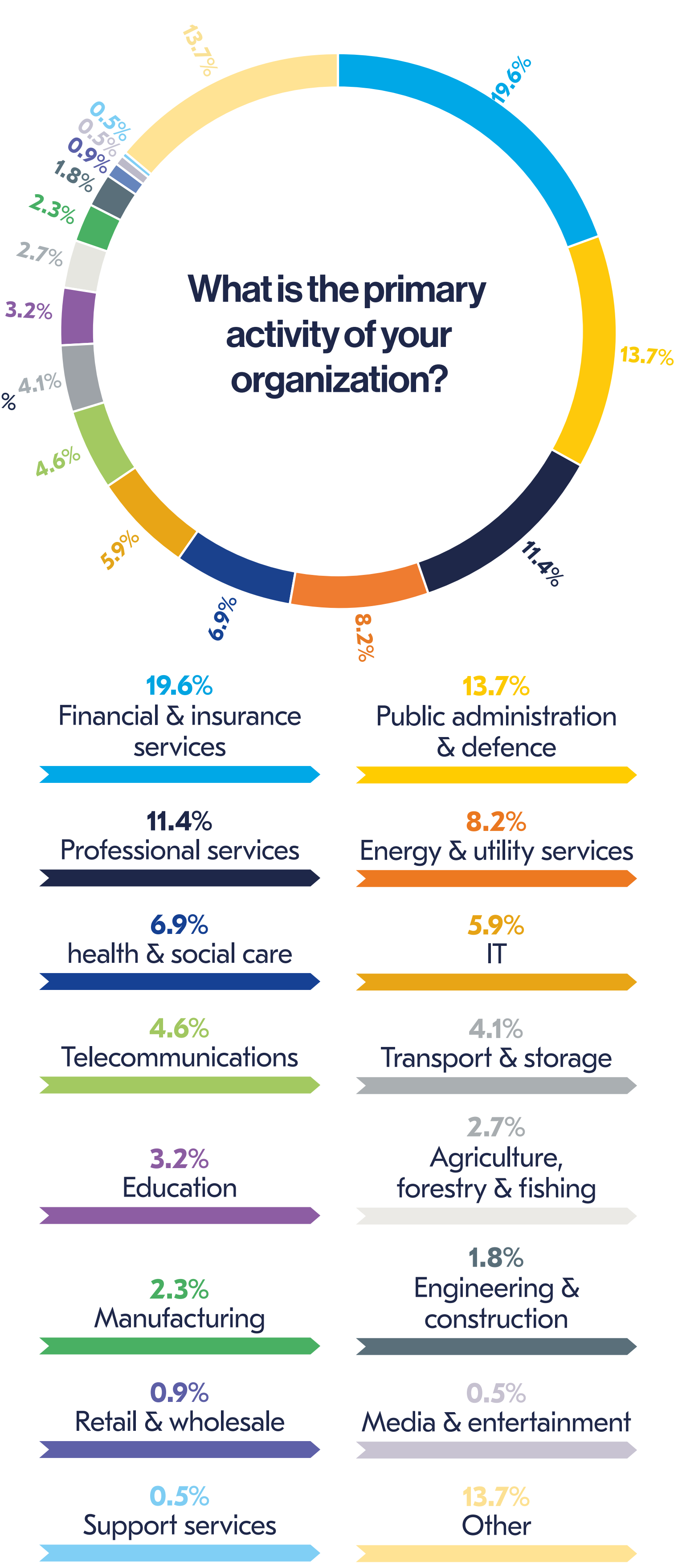


Figure 44. Which region are you currently based in?

Figure 45. What is the primary activity of your organization?

Approximately how many employees work at your organization?

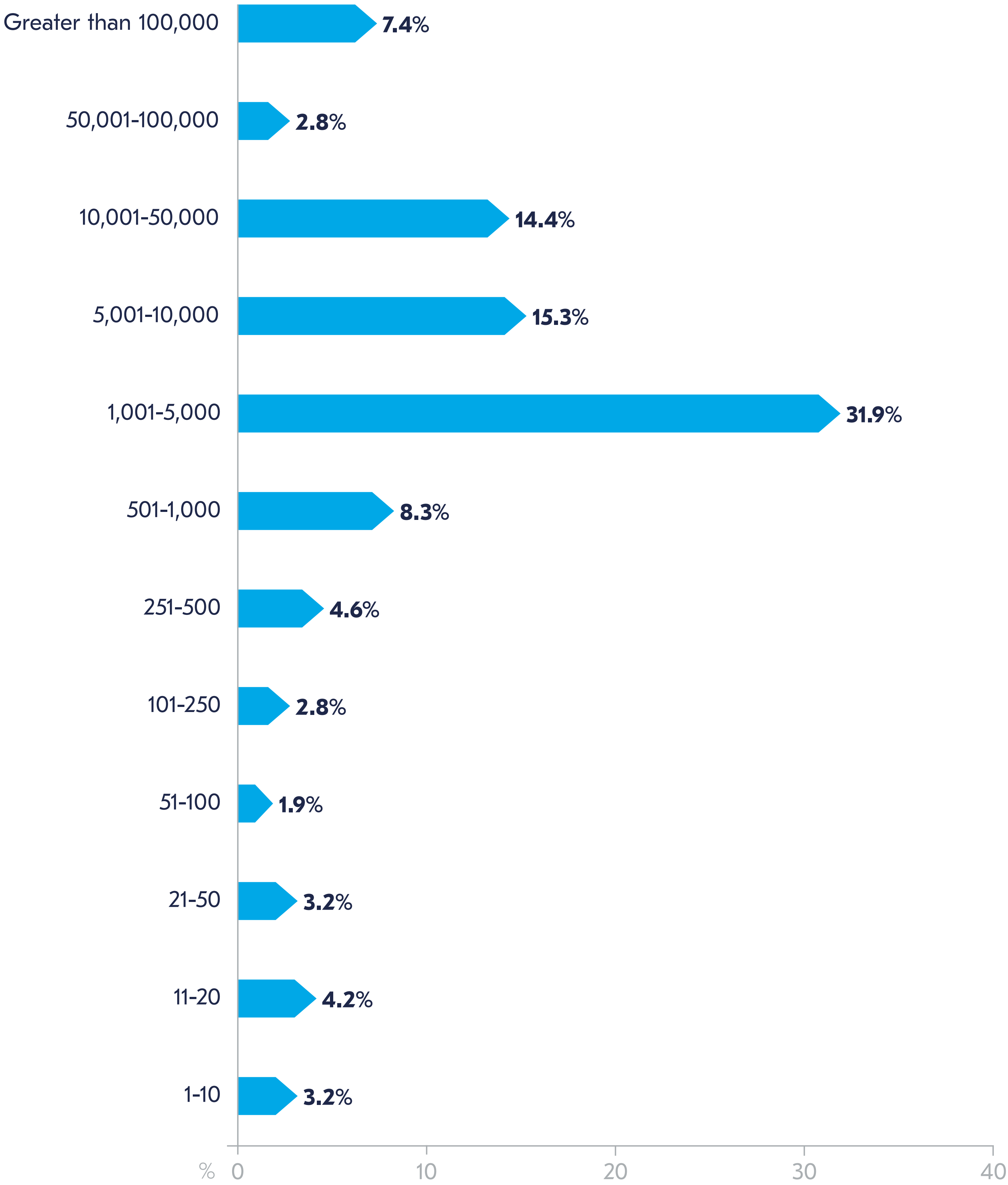
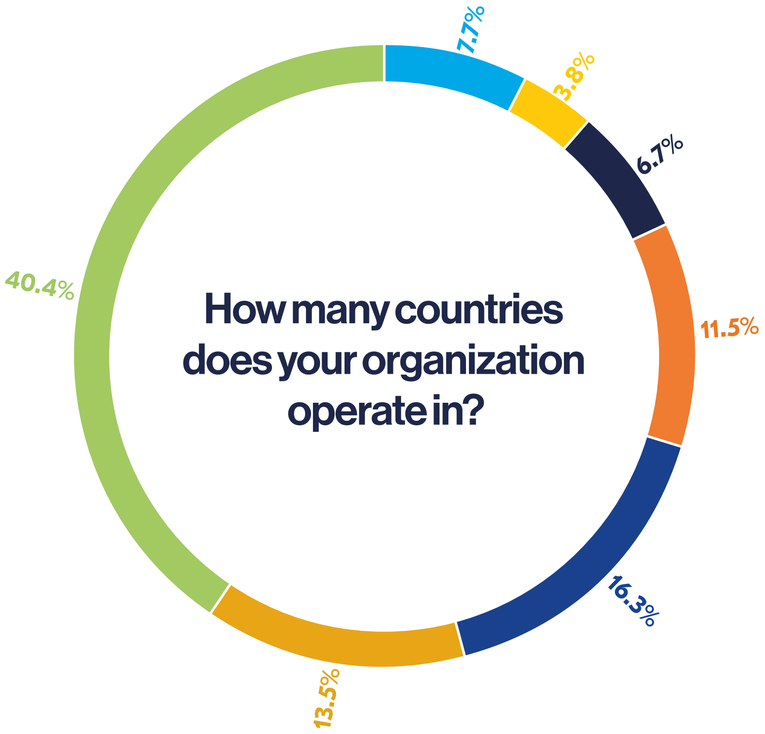


Figure 46. Approximately how many employees work at your organization?



7.7%	1
3.8%	2-4
6.7%	5-10
11.5%	11-25
16.3%	26-50
13.5%	51-100
40.4%	Over 100

Figure 47. How many countries does your organization operate in?

About the authors

Rachael Elliott

(Head of Thought Leadership, The BCI)

Rachael has twenty years' experience leading commercial research within organizations such as HSBC, BDO LLP, Marakon Associates, CBRE, and BCMS. She has particular expertise in the technology and telecoms, retail, manufacturing, and real estate sectors. Her research has been used in Parliament to help develop government industrial strategy and the BDO High Street Sales Tracker, which Rachael was instrumental in developing, is still the UK's primary barometer for tracking high street sales performance. She maintains a keen interest in competitive intelligence and investigative research techniques.

She can be contacted at rachael.elliott@thebci.org

Maria Florencia Lombardero Garcia

(Research Manager, The BCI)

Maria has over 15 years of experience in academic and market research and has been responsible for the design and implementation of a wide range of policies within public and private organizations such as the Argentine Ministry of Defence, RESDAL, and BMI (Fitch Group). She has served as a policy advisor and political analyst at the Argentine Ministry of Defence and coordinated the Argentine National Security Council's Office. She has particular expertise in geopolitical risk, defence, and intelligence and her work has been applied to develop government defence strategies and draft legislation on the matter. Her areas of interest relate to open-source research and how geopolitics impacts resilience within organizations.

She can be contacted at maria.garcia@thebci.org

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the BCI has established itself as the world's leading institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for business continuity and resilience professionals globally with over 9,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public, and third sectors. The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development, and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 partners worldwide, the BCI Corporate Membership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals, and organizations. Further information about The BCI is available at **www.thebci.org**.

Contact The BCI
+44 118 947 8215 | bci@thebci.org
9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK

About F24

F24 is Europe's leading software-as-a-service (SaaS) provider for resilience. More than 5,500 customers worldwide rely on F24's digital solutions, which support companies and organizations through all areas of resilience. Solutions cover business messaging and service notification, emergency and mass notification, incident and crisis management, as well as governance, risk, and compliance.

Multi-sector trust based on over 20 years of experience

F24 supports customers in virtually every sector ranging from energy, healthcare, industry, finance, IT, tourism, and aviation to a wide variety of public organizations. Many years of international experience have made F24 experts in improving resilience with digital solutions.

The company was founded in 2000 in Munich, where F24 AG's head office is still located. Today, F24 supports companies and organizations in more than 100 countries, via more than 20 locations in Europe and beyond. The F24 AG Board of Directors consists of F24 co-founder Christian Götz and the spokesperson Dr. Jörg Rahmer.

In July 2020, Europe's leading software investor Hg became the majority shareholder in F24 AG. Since then, F24 has continued to grow through the second phase of its buy-and-build strategy to further accelerate growth and expand its position as the market leader in Europe.

Recommended by analysts and ISO certified multiple times

In 2018, F24 was the first company based in Europe to be listed in the Gartner report for Emergency and Mass Notifications Systems (EMNS) and meet the stringent requirements of this prestigious institute. In addition, F24 was included in the Forrester Wave™: Critical Event Management Platforms Q4 2023, which looks at 'The 10 Providers That Matter Most And How They Stack Up'. This makes F24 one of the most relevant resilience providers worldwide.

Security is a top priority for F24, which is why the highest and most up-to-date safety standards are in place. In 2010, F24 became the first company worldwide to have their Integrated Management System for Information Security (ISMS) and Business Continuity (BCMS) certified by The British Standards Institution (BSI). Since then, F24 AG and most of its subsidiaries have been certified to ISO/IEC 27001 and ISO 22301 standards. In addition to annual audits by an independent accredited institution, successful re-certifications to the international standards ISO/IEC 27001:2013 and ISO 22301:2019 took place in 2013, 2016, 2019, and 2022.

References

1. https://www.thebci.org/resource/bci-emergency-communications-report-2023.html
2. https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html
3. https://www.thebci.org/resource/bci-emergency-communications-report-2023.html
4. https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html
5. https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html
6. The transition from voice services (PSTN/ISDN) to all-IP technology and the discontinuation of conventional analogue telephony is referred to as the "PSTN switch-off."
7. https://www.analysysmason.com/research/content/data-set/wireline-decommissioning-tracker-rdfi0/
8. https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html
9. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/ishybridworkingheretostay/2022-05-23
10. https://commercialobserver.com/2021/09/40-of-office-workers-worldwide-have-returned-to-in-person-work-report/#:~:text=Despite%20companies%20pushing%20back%20their%20return-to-work%20plans%2C%2040,a%20new%20report%20from%20Cushman%20%26%20Wakefield%20%28CWK%29.
11. https://www.thebci.org/resource/bci-emergency-and-crisis-communications-report-2022.html https://www.thebci.org/resource/bci-emergency-communications-report-2023.html
12. https://faq.whatsapp.com/1623293708131281/?helpref=hc_fnav
13. https://www.thebci.org/resource/bci-emergency-communications-report-2023.html
14. He, E. (2023). Survey: Employees Want Business Technologies to be More Collaborative. Harvard Business Review (online). 23 February 2023. Available at: https://hbr.org/2023/02/survey-employees-want-business-technologies-to-be-more-collaborative (last accessed 2 January 2024)
15. Elliott, R. et al (2023). BCI Horizon Scan Report 2023. 14 November 2023. The BCI (online). Available at: https://www.thebci.org/resource/bci-horizon-scan-report-2023.html (last accessed 3 January 2024)
16. https://www.thebci.org/resource/bci-extreme-weather---climate-change-report-2023.html
17. https://blog.cloudflare.com/radar-2023-year-in-review/
18. https://www.crn.com/news/cloud/the-15-biggest-cloud-outages-of-2023#:~:text=Amazon%20Web%20Services%2C%20Microsoft%2C%20Google,significant%20service%20outages%20this%20year.&text=Technology%20giants%20and%20vendors%20of,for%20running%20critical%20business%20processes.
19. World Health Organization (WHO), The (2022). Infodemics and misinformation negatively affect people's health behaviours, new WHO review finds. WHO. 1 September 2022. Available at: https://www.who.int/europe/news/item/01-09-2022-infodemics-and-misinformation-negatively-affect-people-s-health-behaviours--new-who-review-finds (last accessed 3 January 2024)
20. https://www.globenewswire.com/news-release/2023/03/30/2637841/0/en/Weather-Forecasting-Services-Market-Size-Growing-at-9-4-CAGR-Set-to-Reach-USD-6-1-Billion-By-2032.html
21. https://seismo.berkeley.edu/research/eew_around_the_world.html

BCI 9 Greyfriars Road, Reading, Berkshire, RG1 1NU, UK

bci@thebci.org / www.thebci.org